

NAS Server 4xxx/8xxx

User Guide

Version 5.00

Part Number: 5019.16014

This page is left blank intentionally

Electronic Emission Notice

Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



CE Notice

This device complies with the EMC directive of the European Community and meets or exceeds the following technical standard:

EN 55022 ~ "Limits and Methods of Measurement of Radio interference Characteristics of information Technology Equipment." This device complies with CISPR Class A standard.

<p>Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.</p>
--




Safety Information


To reduce the risk of fire or electric shock, install the unit in a temperature-controlled indoor area free of conductive contaminants. Do not place the unit near liquids or in an excessively humid environment.


Do not allow liquids or foreign objects to enter the unit. All servicing of this equipment must be performed by qualified service personnel. Remove rings, watches and other jewelry before servicing the unit.

Before maintenance, repair or shipment, the unit must be completely switched off and unplugged and all connections must be removed.

Safety Notices:

	<p>The computer may provided with CD drives comply with appropriate safety standards including IEC 60825</p> <div data-bbox="277 443 851 673" style="border: 3px solid black; padding: 10px; text-align: center;"><p>CLASS 1 LASER PRODUCT KLASSE 1 LASER PRODUKT</p></div>
---	---

	<p>Caution: This unit is provided real-time clock circuit. There is a danger of explosion if battery is incorrectly replaced. Replace only with 3-Volt Lithium cell (CR2032) or equivalent type. Discard used batteries according to the manufacturer's instructions.</p>
---	---

	<p>Caution: Before connect or disconnect power cord of the power supply, ensure to turn the power supply switch OFF to avoid the risk of equipment damage.</p>
--	---

This page is left blank intentionally

Table of Content

Chapter 1 Introduction	1
1.1 Features	1
1.2 Conventions	1
Chapter 2 Installing and Starting NAS system	3
2.1 Installing the NAS system controller & MR-423I mobile rack.....	3
2.2 Installing the Mini-Tower Model	11
2.3 Installing the 1U rack-mount Model	13
2.4 Installing the 2U rack-mount Model	17
2.5 Installing the 9-Bay Tower Model.....	18
2.6 Installing the 4U Rack-mount Model	20
2.7 PCI adaptor installation	25
2.8 Setting the IP Addresses.....	27
2.9 Accessing the Administration Home Page.....	32
2.10 Detection of Chassis Intrusion	33
Chapter 3 Server Configuration	35
3.1 Server Information and Settings	35
3.2 Upgrading the Firmware.....	38
3.3 Shutting Down the Server	39
3.4 Enabling UPS Support	41
3.5 Modifying the Administrator's Password	42
Chapter 4 Network Configuration.....	43
4.1 Network Information	43
4.2 TCP/IP Settings.....	45
4.3 Windows Settings.....	47
4.4 UNIX/Linux Settings	49
4.5 Macintosh Settings.....	52

4.6 NetWare Network Settings.....	53
4.7 Web Data Access Settings	54
4.8 FTP Data Access Settings	55
4.9 SNMP Settings.....	56
4.10 Email Settings	58
4.11 SSL Settings	59
Chapter 5 Storage Management	61
5.1 Volume Usage and Status	61
5.2 Creating a Volume	65
5.3 Deleting a Volume.....	66
5.4 Expanding a RAID-5 Volume	67
5.5 SmartExtend – Add More NAS Capacity	68
5.6 Volume/Disk Scan.....	72
5.7 Assigning Hot-spare Disks.....	73
5.8 Hot-swapping	74
Chapter 6 Security Control	77
6.1 Security Information	77
6.2 Creating the Local User and Local Group Accounts...	79
6.3 Caching Windows Domain User Accounts	81
6.4 Creating UNIX/Linux Host.....	83
6.5 Creating Share and Assigning Share Permissions.....	84
6.6 Configuring File and Folder Security and ACL	87
6.7 Managing Quotas.....	92
Chapter 7 Disc Sharing and Data Archiving 95	
7.1 Start to Use the Disc Server Function.....	95
7.2 Creating Disc Images.....	96
7.3 Managing Discs.....	98
7.4 Sharing Discs	99
7.5 Burning Disc Images.....	101
7.6 Archiving Data to CD/DVD Discs	102

Chapter 8 User Access	105
8.1 Workgroup or Domain Mode	105
8.2 Accessing from Windows	107
8.3 Accessing from Web Browsers	109
8.4 Accessing from MacOS.....	112
8.5 Accessing from FTP Clients.....	114
8.6 Accessing from NFS Clients	115
Chapter 9 Backup and Recovery	117
9.1 Snapshot – Fast Point-In-Time Copies	117
9.2 Loading and Writing CD/DVD Discs	121
9.3 Tape Backup and Restore	125
9.4 Using a Tape Library	129
9.5 SmartSync – NAS-to-NAS Data Replication.....	136
9.6 Backup and Restore System Profiles	145
Chapter 10 Event Logs and System Status	147
10.1 Thermal Settings	148
10.2 Checking the Event Logs	149
10.3 Viewing System Status	151
10.4 Saving System Settings and Status as HTML Files	153
Chapter 11 Virus Protection	155
11.1 Information	155
11.2 Real-time, Manual and Schedule Scanning.....	157
11.3 Configuring Scan Settings	159
11.4 Updating Virus Pattern File	161
Chapter 12 Activating Optional Features ..	163
12.1 Activating Optional Features	163
Appendix A Specification.....	165
Hardware Specification for the 5.25" NAS Controller	165
Hardware Specification for 8400M NAS Main board	168

Hardware Specification for MR-423I Hotswap HDD module	172
Hardware Specification for 1U Rack mount Model	173
Hardware Specification for the Mini-Tower Model	175
Hardware Specification for the 9-bay Tower Model	175
Hardware Specification for the 4U Rack Mount Model ...	176
Hardware Specification for the 2U Rack Mount Model ...	176

Appendix B Utility for NAS system 179

Installation	180
Discovering NAS system.....	181
Importing and Exporting System Settings.....	182
Browsing & Administering Servers.....	184
Mirroring CD/DVD Remotely	188
Archiving Files As a CD/DVD Image.....	192
Burning Disc Images	196
Supported CD Formats	196

Chapter 1 Introduction

1.1 Features

The NAS system is a premier NAS product featuring tera-bytes of massive storage capacity and full-range data protection to provide a cost-effective, highly reliable and high-performance storage system for the fast growing network storage demand.

- Deliver storage capacity over tera-bytes
- Expand RAID storage capacity without downtime
- Feature with hot-swappable HDD to maximize storage flexibility
- Accelerate network throughput with the dual-NIC and Gigabit Ethernet support
- Utilize the power management support with UPS
- Seamless integration into heterogeneous networking security
- Backup and archive important data to the local tape drive, CD/DVD writer or a remote storage server

1.2 Conventions

Terminology

The term “NAS system” means all the models of the network-attached storage servers unless the specific model is mentioned.

Typographic Conventions

Conventions	Meaning
-------------	---------

Conventions

<i>Italic</i>	Variable name, which should be replaced by user-defined text in context
Bold	Menu item
Monospaced font	Text which users should type in
<u>Underline</u>	Cross-reference

Chapter 2 Installing and Starting NAS system

This chapter covers the installation procedure of different form factors of NAS system as well as the **MR-423I** Mobile Rack. Instruction on how to startup the NAS system by setting up the basic configuration through the Admin Home page or provided software tool – NASStart is also outlined in this chapter.

2.1 Installing the NAS system controller & MR-423I mobile rack

Package Contents

NAS system controller package:

- NAS system controller unit with one PCI riser card
- Daughter board A – two RJ-45 ports and one serial connector
- Daughter board B – one RJ-45 port (Optional for Gigabit Ethernet)
- Four flat IDE cables
- One tubular IDE cable for ATAPI devices
- Three Ethernet cables
- One 10-pin serial cable*
- NAS system user guide
- NAS system utilities CD

* Pre-installed on the controller unit

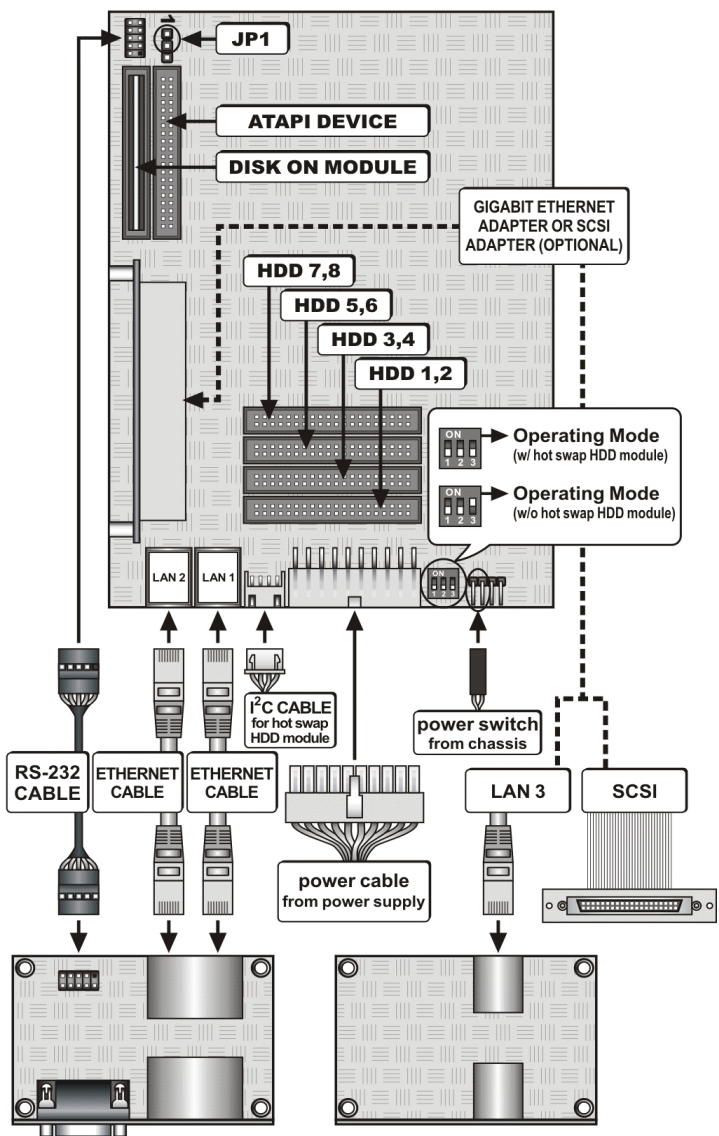
MR-423I mobile rack package:

- One mobile rack that holds 4 hard disks and fit into 3x5.25" drive bays
- Two tubular IDE cables

- One I²C cable

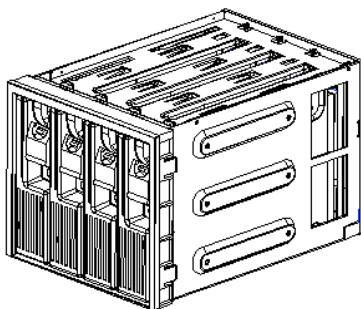
Connecting the cables on the NAS system controller

Refer to the following diagram to connect all the cables provided along with the package.



Install NAS system controller with MR-423I mobile rack

You can get the benefits from the full-range data protection with hot-swappable hard disks by installing the MR-423I mobile racks with the NAS system controller.



The MR-423I can be configured to operate in two modes by configuring the jumper (J11) at the rear side of the mobile rack:

J11	1-2	2-3
Master and Slave Mode	Short	Open
All Master Mode	Open	Short

In **Master and Slave Mode**, each IDE connector on the mobile rack can support two hard disks. In other words, it allows two hard disks using the same IDE cable and arranges the hard disks as a Master drive and Slave drive.

In **All Master Mode**, each IDE connector on the mobile rack can support only one hard disk and that become the Master drive. It is recommended that configure the MR-423I to **All Master Mode** only when one MR-423I is used on the system.

The following conditions are required for the NAS system controller and MR-423 mobile rack install to your server chassis:

- Using the provided IDE tubular cables to connect to the mobile rack from controller is required.
- Configuring the DIP switches at the rear side of your NAS system main board to **1:OFF 2:OFF 3:OFF**

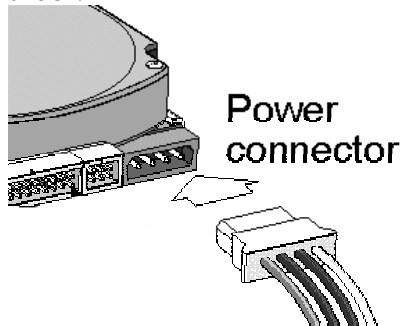
Installing the NAS system controller & MR-423I mobile rack

- Configuring the jumper on your hard disk using Cable Select (CS) before install to the hard disk tray of the MR-423I mobile rack. (Refer to your hard disk's user manual for the instruction)
- Configuring the jumper (J11) on the rear of the MR-423I mobile rack to either the **Master and Slave Mode** or **All Master Mode**.
- Make sure that the all your mobile racks and the NAS system controller are linked by the I²C cable provided.
- Two power connectors are required for each MR-423I mobile rack.

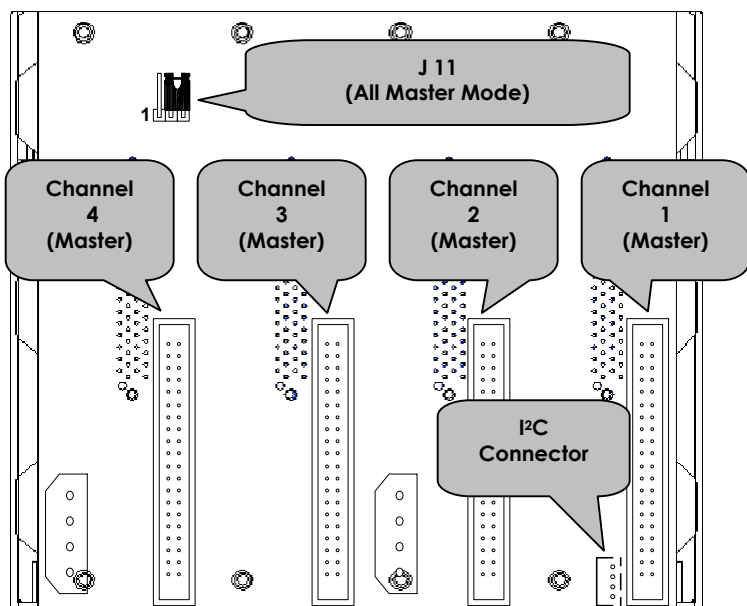


Caution:

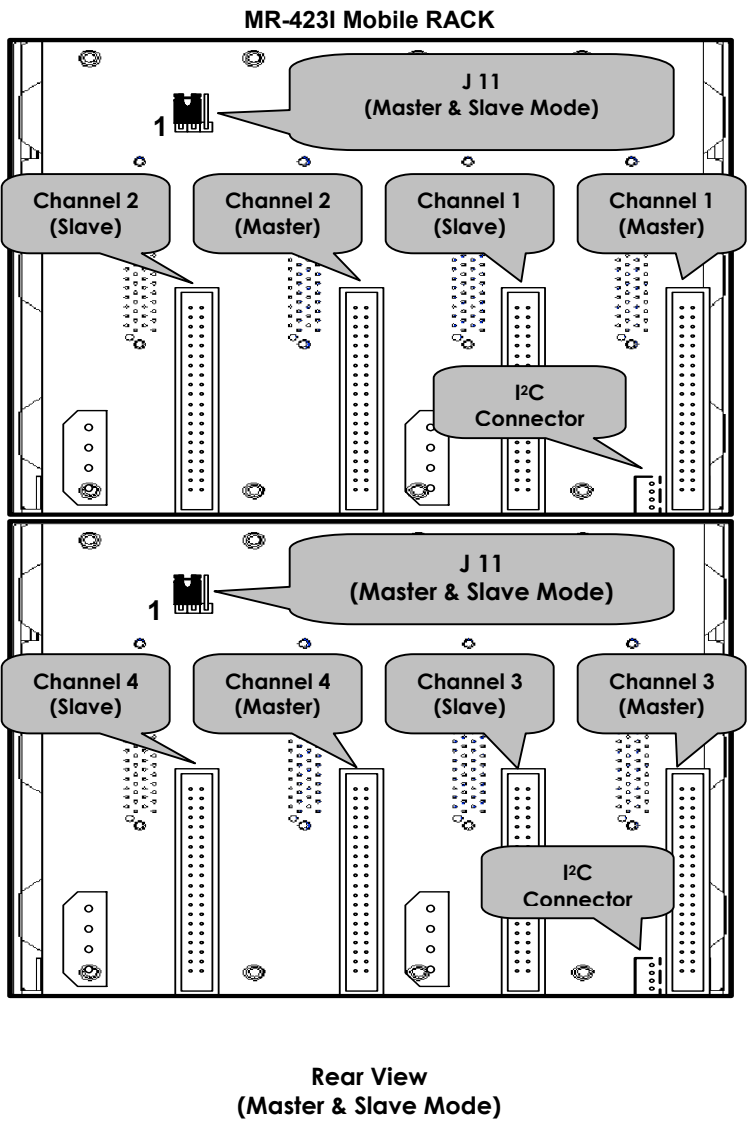
When connecting the power connector to the MR-423I or HDD, the connector has rounded edges on the top of the connector that should be placed in the proper position to avoid equipment damage or electric shock.



MR-423I Mobile Rack



**Rear View
(All Master Mode)**



Install NAS system controller without MR-423I mobile rack

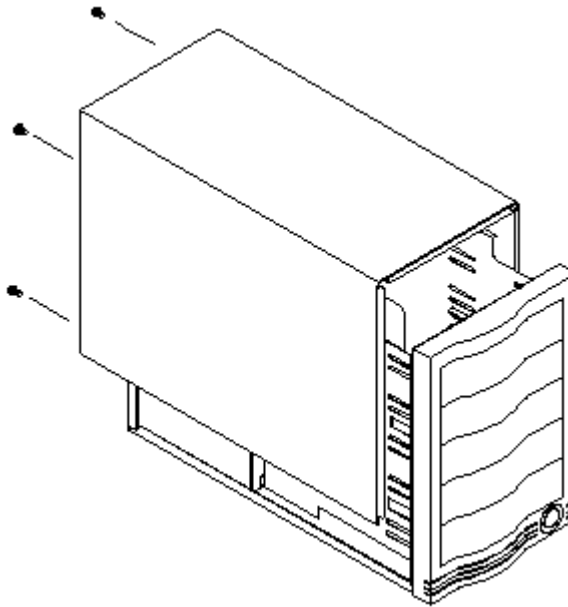
You will not have the benefits of the full-range data protection with hot-swappable hard disks if the MR-423I mobile rack is not installed in your system.

The following conditions are required for the NAS system controller installed to your server chassis:

- Using the bundled IDE flat cables to connect to the hard disks from controller is required.
- Configuring the DIP switches at the rear side of your NAS system main board to 1:OFF 2:OFF 3:ON
- Configuring the jumper on your hard disk using Master or Slave only. (Refer to your hard disk's user manual for the instruction)

2.2 Installing the Mini-Tower Model

In the tower model, NAS system controller and the **MR-423I** mobile rack (no HDD installed) are pre-installed before shipping.



Package Contents

A mini-tower system comes with the following items:

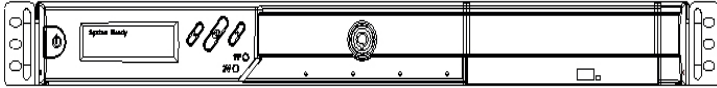
- Mini-tower chassis
- NAS system controller unit
- One MR-423I mobile racks
- Daughter board A – two RJ-45 ports and one serial connector
- ATX power supply

- NAS system user guide
- NAS system utilities CD

Tower installation

1. Pull out a HDD tray from the **MR-423I** mobile rack.
2. Configuring the jumper on your hard disk using Cable Select (CS) before installing to the hard disk tray. (Refer to your hard disk's user manual for the instruction)
3. Secure and mount a hard disk onto the HDD tray using four screws under the tray.
4. Insert the HDD tray back in the mobile rack. Make sure the lever of the mobile rack is properly in place.
5. Repeat Step 1 to Step 3 if necessary for the other HDD trays.
6. Connect your NAS system to the network by attach a LAN cable from the LAN port located at the back of your NAS system. (At least one network connection is required)
7. Plug the power cord into the power connector on you NAS system.
8. Make sure the power switch on the power supply is in **ON** position.
9. Press the power button on the upper right hand corner of your NAS system.
10. Wait for the server to boot up. The boot up process takes approximately 2 minutes.

2.3 Installing the 1U rack-mount Model



Package Contents

A 1U rack-mount system comes with the following items:

- 1U rack-mount server
- DVD combo drive (optional)
- 28" rack mount sliding rail kit
- Screws for HDD mounting
- Key for the front bezel lock
- NAS system user guide
- NAS system utilities CD

Hot swap hard disk tray installation

1. To unlock the hot swap hard disk tray, pull the tab behind the end of the lever to release the latch and then lift the lever up as far as it can go to disengage the hard disk tray from the chassis.

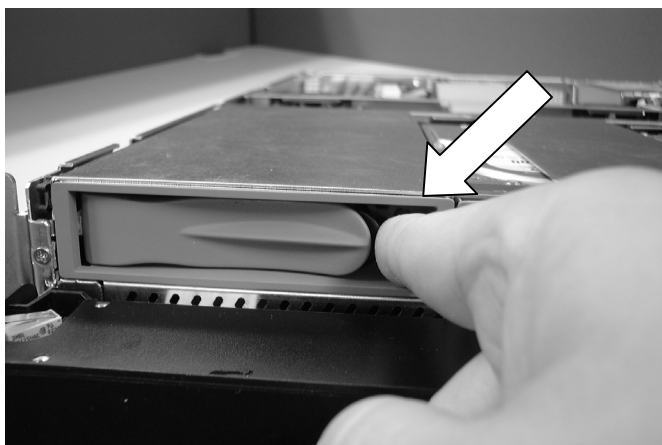


Figure 1

2. Pull the hard disk drive tray out.
3. Attached the HDD to the hot swap hard disk tray with the screws provided shown in Figure 2.

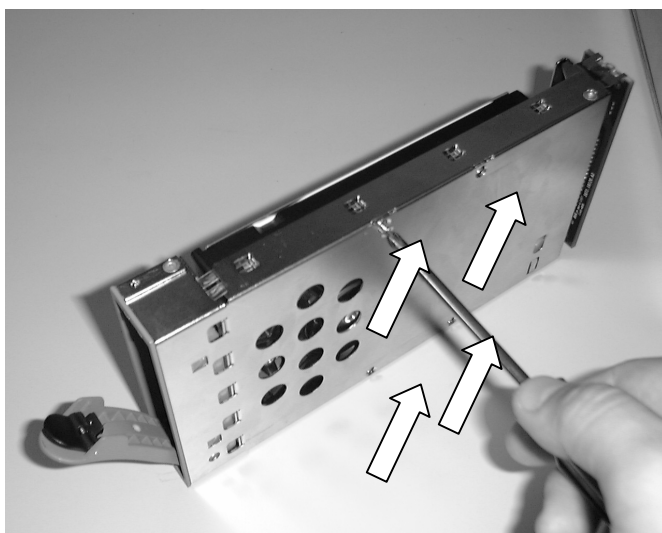


Figure 2

4. Slide the hot swap hard disk tray slowly into the chassis, push the outer rim of the tray as shown in Figure 3 until the lever retract slowly toward the tray. Then, push the level down as far as it can go to connect the hot swap hard disk tray to the chassis.

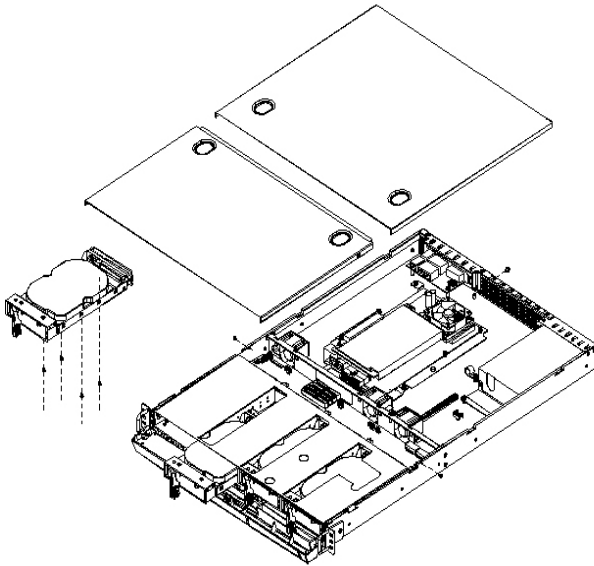


Figure 3

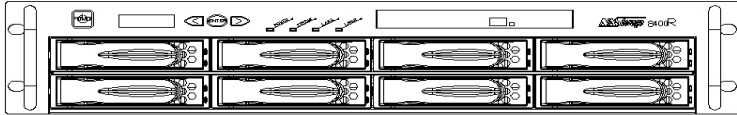
1U rack-mount server installation

1. Pull out a HDD tray from the server.
2. Configuring the jumper on your hard disk using Cable Select (CS) before installing to the hard disk tray. (Refer to your hard disk's user manual for the instruction)
3. Secure and mount a hard disk onto the HDD tray using four screws under the tray.
4. Insert the HDD tray back in the server. Make sure the lever of the HDD tray is properly in place.
5. Repeat Step 1 to Step 3 if necessary for the other HDD tray.
6. Install the provide rack mounting handles at both side of the NAS system.
7. Install the NAS system in the rack. (Refer to the paragraph "Sliding Rails Installation" in Chapter 2 section 5)

8. Connect your NAS system to the network by attach a LAN cable from the LAN port located at the back of your NAS system.(At least one network connection is required)
9. Plug the power cord into the power connector on you NAS system.
10. Make sure the power switch on the power supply is in on position.
11. Press the power button on the left hand corner of your NAS system.
12. Wait for the server to boot up. The boot up process takes approximately 2 minutes.



2.4 Installing the 2U rack-mount Model



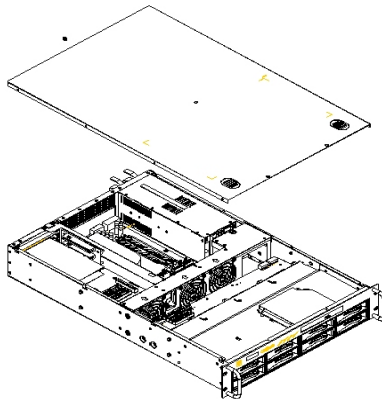
Package Contents

A 2U rack-mount system comes with the following items:

- 2U rack-mount server
- DVD combo drive (optional)
- 28" rack mount sliding rail kit
- Screws for HDD mounting
- NAS system user guide
- NAS system utilities CD

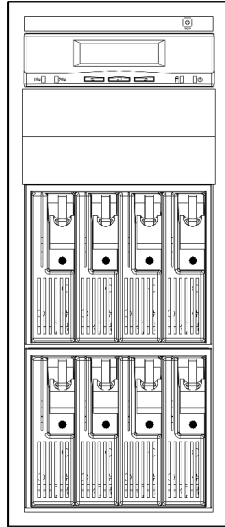
Hot swap hard disk tray installation

(Refer to the paragraph "Sliding Rails Installation" in Chapter 2 section 6)



2.5 Installing the 9-Bay Tower Model

In the tower model, NAS system controller and the **MR-423I** mobile rack (no HDD installed) are pre-installed before shipping.



Package Contents

A 9-Bay tower system comes with the following items:

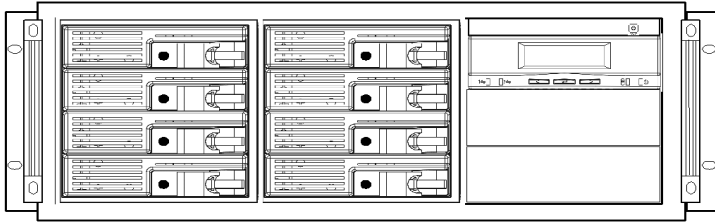
- 9-Bay tower chassis
- NAS system controller unit with one PCI riser card
- Two MR-423I mobile racks
- Daughter board A – two RJ-45 ports and one serial connector
- Daughter board B – one RJ-45 port (Optional for Gigabit Ethernet)
- Single or redundant ATX power supply
- NAS system user guide
- NAS system utilities CD

Tower installation

1. Pull out a HDD tray from the **MR-423I** mobile rack.
2. Configuring the jumper on your hard disk using Cable Select (CS) before installing to the hard disk tray. (Refer to your hard disk's user manual for the instruction)
3. Secure and mount a hard disk onto the HDD tray using four screws under the tray.
4. Insert the HDD tray back in the mobile rack. Make sure the lever of the mobile rack is properly in place.
5. Repeat Step 1 to Step 3 if necessary for the other HDD trays.
6. Connect your NAS system to the network by attach a LAN cable from the LAN port located at the back of your NAS system.(At least one network connection is required)
7. Plug the power cord into the power connector on you NAS system.
8. Make sure the power switch on the power supply is in **ON** position.
9. Press the power button on the upper right hand corner of your NAS system.
10. Wait for the server to boot up. The boot up process takes approximately 2 minutes.

2.6 Installing the 4U Rack-mount Model

In the 4U rack model, NAS system controller and the **MR-4231** mobile rack (no HDD installed) are pre-installed before shipping.



Package Contents

A 4U rack mount system comes with the following items:

- 4U rack mount chassis with two rack-mounting handles
- Sliding rails (optional)
- NAS system controller unit with one PCI riser card
- Daughter board A – two RJ-45 ports and one serial connector
- Daughter board B – one RJ-45 port (optional for Gigabit Ethernet)
- Single or redundant ATX power supply
- NAS system user guide
- NAS system utilities CD

4U Rack installation

1. Pull out a HDD tray from the **MR-4231** mobile rack.
2. Configuring the jumper on your hard disk using Cable Select (CS) before installing to the hard disk tray. (Refer to your hard disk's user manual for the instruction)
3. Secure and mount a hard disk onto the HDD tray using four screws under the tray.

Installing the 4U Rack-mount Model

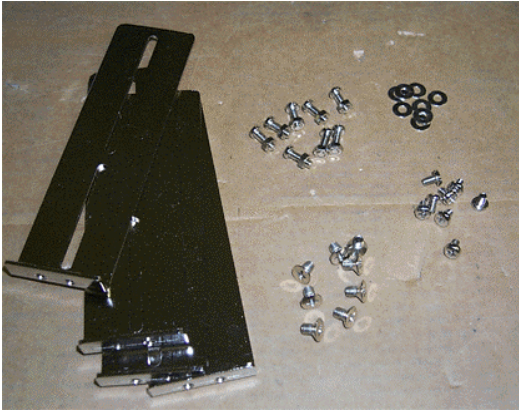
4. Insert the HDD tray back in the HDD module. Make sure the lever of the HDD module is properly in place.
5. Repeat Step 1 to Step 3 if necessary for the other HDD tray.
6. Install the provide rack mounting handles at both side of the NAS system.
7. Install the NAS system in the rack.
8. Connect your NAS system to the network by attach a LAN cable from the LAN port located at the back of your NAS system.(At least one network connection is required)
9. Plug the power cord into the power connector on you NAS system.
10. Make sure the power switch on the power supply is in on position.
11. Press the power button on the upper right hand corner of your NAS system.
12. Wait for the server to boot up. The boot up process takes approximately 2 minutes.



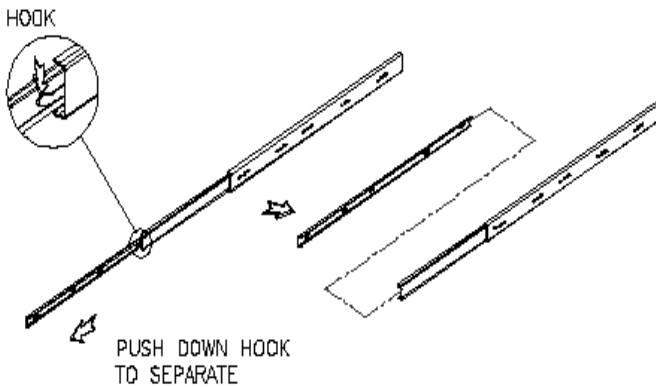
Note: It is recommended that rear support bracket on the cabinet should be used when installing the 4U rack model

Sliding Rails Installation

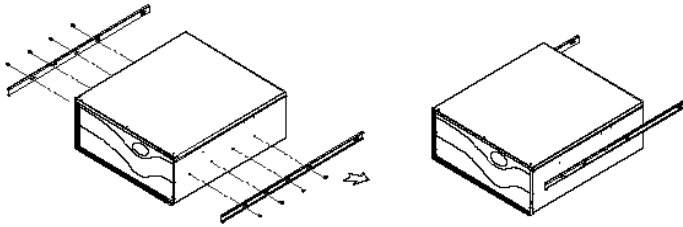
1. Make sure that you have the following the mounting parts for the sliding rails.
 - 4 L-shaped brackets (see the left side of the photo)
 - 8 long screws and washers (see the upper right side of the photo)



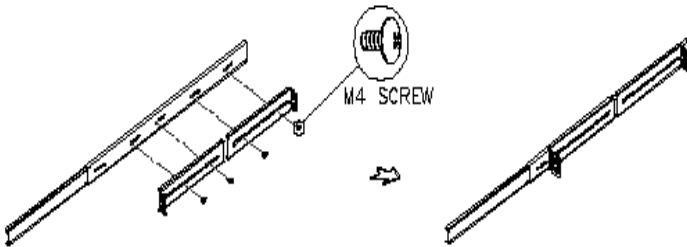
2. Take the sliding rail apart by sliding out the center slide. Push down the hook to separate them. Pull the center slide all the way until it reaches the end.



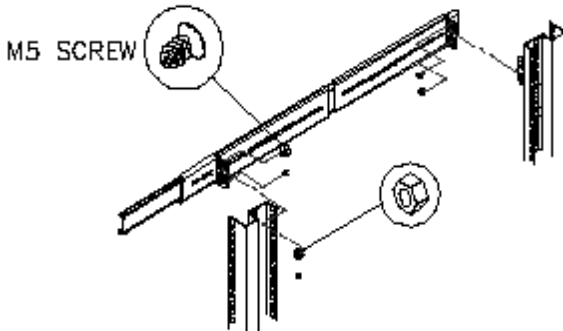
Now install the center slide to the rack-mount chassis. Find the screw holes on both sides of the rack-mount chassis, which are used for mounting the center slide. Fasten the 8 screws to fix the center slides onto chassis. Later, the center slides will be used for attaching to the sliding rail.



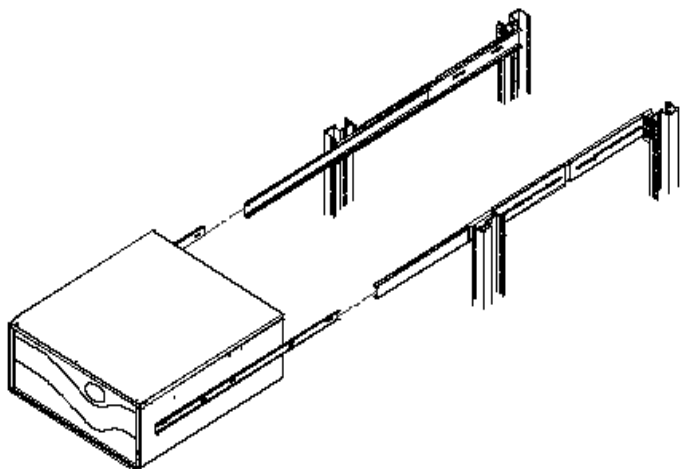
3. Next, attach the two L-shaped mounting brackets on to a sliding rail. Use the M4 screws to secure the L-shaped bracket on to the sliding rail.



Attach the sliding rail onto a rack-mount cabinet. Secure the sliding rail onto the rack-mount cabinet via the screw holes on the L-shaped brackets.



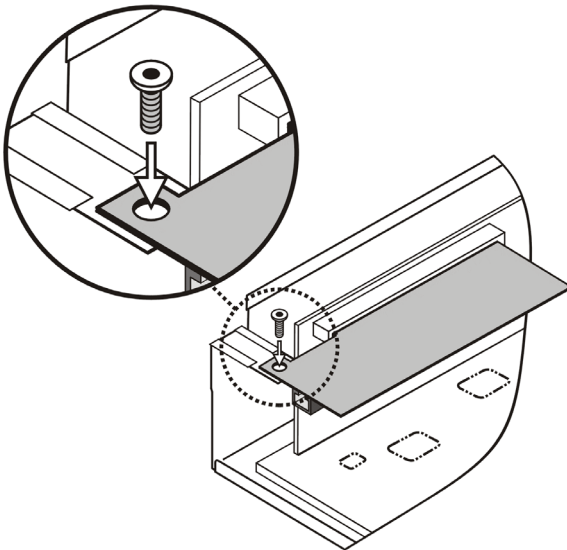
4. After properly attaching both sliding rails to the rack-mount cabinet, you may slide the rack-mount chassis (mounting) in to the cabinet.



2.7 PCI adaptor installation

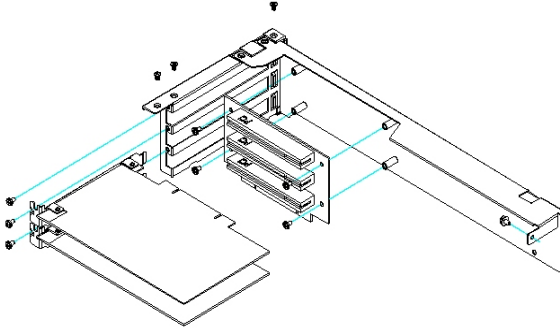
For controller:

1. Turn off your NAS system and unplug it from the wall
2. Open the server case
3. Remove the screws from both sides of the NAS system controller unit. Put the controller unit in a position that you can insert the PCI adaptor into the on-board PCI slot
4. When the PCI adaptor is installed, secure it as shown on the following diagram.



5. Connect cable for the PCI adaptor at the inner back of the server case.
6. Secure the controller unit via the screws holes on both sides
7. Close your server case and plug in your power cable
8. Turn on the NAS system
9. Your PCI adaptor is now be installed

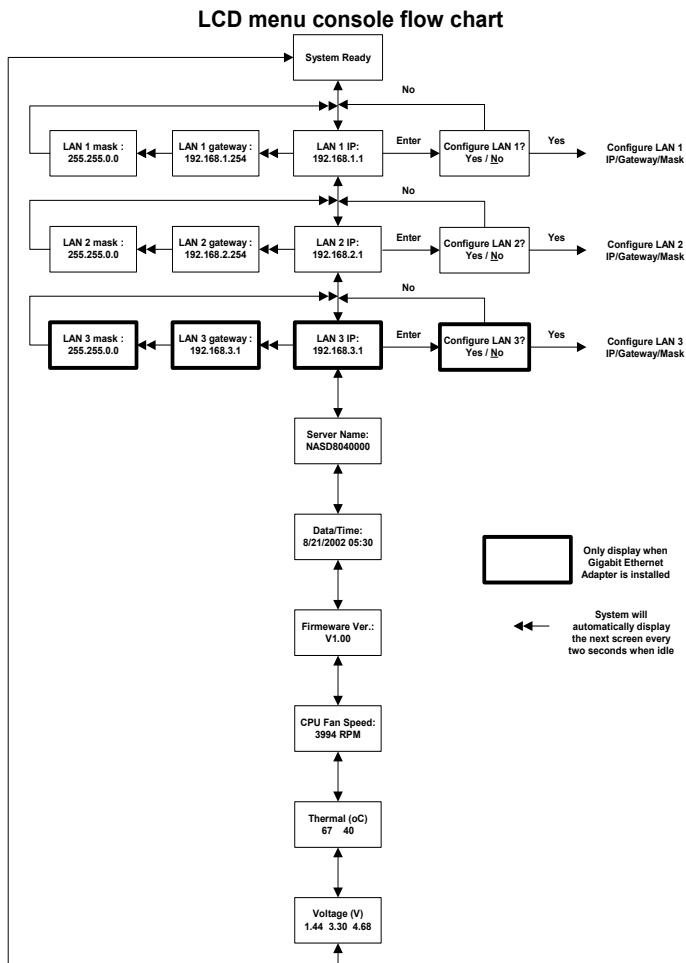
For 2U rack mount server:



1. Turn off your NAS system and unplug it from the wall
2. Open the server case
3. Loosen the screws and remove the riser card support bracket
4. Place the adaptor, component-side down, and press the adaptor firmly into one of the PCI slot on the riser card
5. Tighten the screw for the adaptor
6. Reinstall the riser card support bracket and make sure that the riser card is fully seated in the PCI slot on the main board
7. Tighten the screw for the riser card support bracket
8. Close your server case and plug in your power cable
9. Turn on the NAS system
10. Your PCI adaptor is now be installed

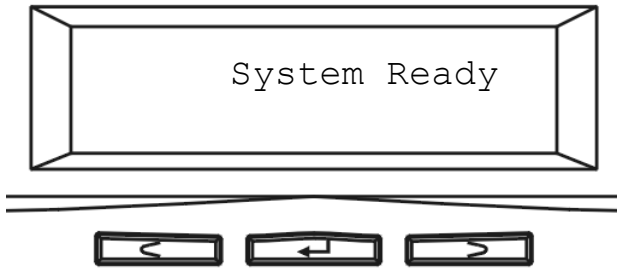
2.8 Setting the IP Addresses


LCD console flow chart

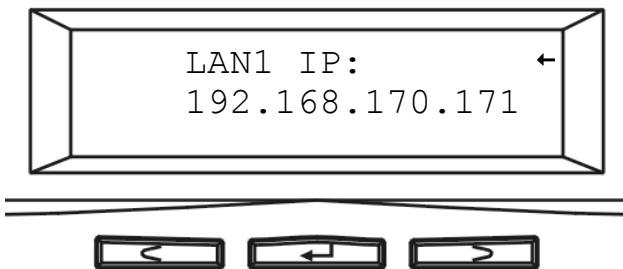


Configuring the IP addresses using the LCD console

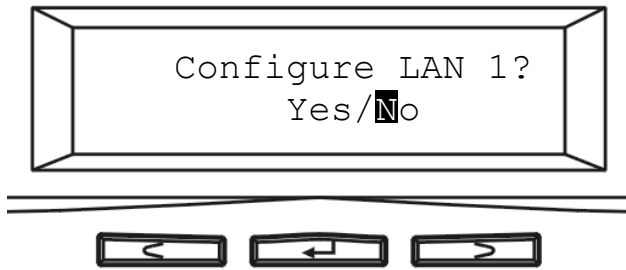
1. After NAS system is boot up, the LCD console shows **System Ready**. Press the right button.



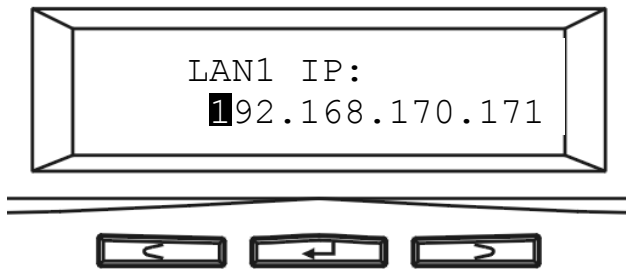
2. The IP address of LAN1 is shown. Press the middle button to configure LAN1 IP address. Note that the  symbol at the right hand upper corner indicates that the IP address can be configured using the LCD console.



3. Move the cursor to **Yes** by pressing the left button and then press the middle button to confirm.



4. Move the cursor to the correct position using the left or right button. Then press the middle button to change that number.




5. After you edit the last digit of the IP address, press the right button and configure the **Subnet Mask** address.
6. Repeat Steps 4 to Steps 5 to configure the **Subnet Mask** and **Gateway** address.
7. After you edit the last digit of the **Gateway** address, press the right button. Move the cursor to **Save** and save the setting or **Edit** to repeat the above process or **Abort** to quit the configuration process without saving.



8. Repeat the above process to configure the other LAN port.

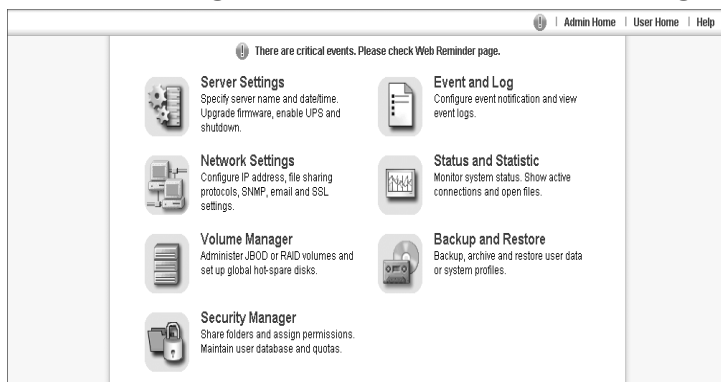
Configuring the IP addresses using NASTart

You can use the provided utility NASTart to perform the initial setup of your newly arrived NAS system. The utility designed to perform a quick set up and put your NAS system online in just a few minutes. During startup, NASTart begins to discover all the NAS system on the network. The default server name would be **NASxxxxxxx**, where **xxxxxxx** is the last eight digits of the Ethernet address of LAN1.

1. Highlight the server you want to configure from the left hand pane.
2. Click the  button on the toolbar
3. Or, right click the server and select **Configure...**
4. Enter the **Server Name**, **Server Comment**, and **Workgroup/Domain Name** and select either the **Workgroup mode** or **Domain mode**.
5. Click **Next** button to go to the next page.
6. Choose the **Network Teaming Mode** from the pull down menu. If you are not clear about this feature, continue with the default value.
7. If you want IP settings to be assigned automatically, click **Obtain IP settings automatically**.

8. Or, you can specify IP settings manually.
9. Click **Next** button to go to the next page.
10. Change the admin password if necessary.
11. Click the **Finish** button to save the settings. Note that server may need to reboot for certain parameters changes to take effect.

2.9 Accessing the Administration Home Page



You can configure the detail settings of your NAS system in the administration home page. To access the administration home page of NAS system, type the URL name of your NAS system in the address field of the web browser:

`http://192.168.1.1 /admin/` , or

Run the utility **NASstart** provided in the CD-ROM, right-click on a NAS server on the left-hand tree-view pane. Select **Admin page** item from the right-click menu to open the administration page. It will prompt for username and password. By factory default, the username is **admin** and no password is needed.



Note: It is recommended that user change the admin password immediately to keep your NAS system secure and to protect resources from inappropriate access by other users on the network.

2.10 Detection of Chassis Intrusion

Model 4400/8400 supports the detection of chassis intrusion and door intrusion. When the chassis is opened or chassis door is opened, the system will send email alerts or SNMP traps. To enable the function, please go to the **Event→Configuration** menu on the administration page. Click the **Advanced** button and check the **Chassis intrusion detected** item.

Please refer to the 8400M specifications in Appendix A - Specification for the pins on the motherboard to which the sensors should be connected. Please note that the sensor must be connected to the main boards correctly for the function to work.

This page is left blank intentionally

Chapter 3 Server Configuration

This chapter describes how to name the server, specify the server date and time, upgrade the OS firmware, shut down the system and use UPS with the NAS system.

3.1 Server Information and Settings

Click **Server** from the administration homepage. You will see the **Information** page describing the summary information of the NAS system.

The **Information** page is divided into two sections. The **General Settings** section shows the parameters which can be modified on the **Server→General** page.

Server Name	Name of the NAS system. A NAS system has one unique name, applicable to all network protocols.
Server Comment	The text which is shown in the comment field when browsing network computers in Windows Network Neighborhood
Date/Time	Server date and time in 24-hour format
Time Zone	The time zone setting of the server relative to the Greenwich standard time
Language (Codepage)	The language used by the server to interpret the server name, user names, share names, file names, etc. Technically, it specifies the codepage which is used to interpret the characters.
CP437-DOSLatinUS: Latin characters	

	for the United States CP850-DOSLatin1: Latin characters for West European CP932-Shift JIS: for Japanese CP936-Chinese GB: for Simplified Chinese CP949-Unified Hangul: for Korean CP950-Chinese Big5: for Traditional Chinese Mac Roman: Latin characters for Macintosh
Configure from LCD	Indicates whether users can configure the server from the LCD console
System LCD Banner	Indicates the banner text which is displayed on the LCD console when it receives no user input or event messages for a period of time
UPS Support	Indicates whether the UPS support is enabled or not
Auto Power Restoration	If enabled, the server will power on automatically when the power restores after abnormal shutdown
System folder resides in	Display the volume name of which the system folder is located

The **System Information** section shows the hardware and firmware status of the server.

Firmware Version	The version number of the OS firmware
Processor Speed	The CPU operating frequency
Memory Capacity	The total size of the main memory
No. of HDD/CD/tape	Display the number of HDD/CD/tape installed in the system
LAN1/2/3 Ethernet Address	The Ethernet MAC addresses of the network controller chips and their types

PCI Slot	Display the type of the add-on adaptor installed in the system
-----------------	--

3.2 Upgrading the Firmware

Updating OS firmware will accommodate new functions or bug-fixes. Once you get new releases of an OS firmware image, you can upgrade the OS firmware by using the web browser. The process is simple and fast.

Once you get the image file of the new OS firmware from your vendor, open the **Administration Homepage** of the NAS system and select the **Server→Upgrade** menu. Specify the full path of the image file or click the **Browse...** button to find it. Click **Apply** to begin. The process might take several minutes. The server will reboot after the firmware is upgraded.

3.3 Shutting Down the Server

Shutdown, reboot and startup actions

The NAS system can be shut down by pressing the power button at the front of the server case. The whole shutdown process might take seconds to minutes until data are all safely saved to the hard disks.

To shut down the server from the **Administration Homepage**, select **Shutdown** from the **Server** menu and click the **Reboot** or **Shutdown** button.

You can specify the actions to take during the next startup.

Recalculate user quota information	Recalculate the storage consumption per user during the next startup. It may take much time if there are a huge amount of files in disk.
Reset configuration to factory default	Reset the server settings, network settings and event configuration to factory default during the next startup. The settings related to the storage, like shares, ACLs, user database, will not be cleared.

Scheduled shutdown and power-on

To set the automatic power-on and shutdown schedules, select the **Server→Shutdown** menu. Click the **Schedule** tab to modify the schedules.

On the schedule settings page, you can set daily or day of month schedules. Check the **Enable** check-boxes and specify

Shutting Down the Server

the time of powering on or shutting down. Remember to click the **Apply** button to submit the changes.

3.4 Enabling UPS Support

The NAS system supports UPS and basic power management functions. It sends alerts when there are power events like utility power failure or low battery capacity. When power events occur, the NAS system can shut down itself automatically to prevent potential data loss.

To use smart-signaling UPS, connect UPS to the NAS system with an RS-232 cable. Then go to the **Server→UPS Settings** menu on the administration page to enable UPS support.

To use network-type UPS, connect the UPS to the LAN first. Then go to the **Server→UPS Settings** page on the administration page. Enable UPS support, select **Network UPS** from the **UPS Type** menu and enter the UP IP address below.

Below are the shutdown options on the page.

Shut down immediately when battery is low	Specify whether to shut down the server when UPS battery is low. Note: When utility power fails, the NAS system will always shut down.
Shut down in x minutes when AC fails	Specify how many minutes to wait before shutting down the server when a power event occurs.
Turn off UPS when shut down by power failure	If checked, the NAS system will turn off the UPS while it is shutting down by power failure. If not, the UPS will still be working when the server is shut down.

3.5 Modifying the Administrator's Password

Admin is a built-in user account for the administrator. It is like the **root** account in UNIX or the **administrator** account in Windows 2000 or XP. Using this account, users have access to the administration homepage and all the storage resources. By default, the password for this user account is empty. To prevent security vulnerability, it is strongly suggested to specify the password when performing the first-time setup of the NAS system.

To specify or modify the administrator's password, please select the **Server→Password** menu on the administration homepage. Input the current admin password in the **Old Admin Password** field, and the new password in the **New Admin Password** and **Confirm Admin Password** fields. Then click **Apply**.

The administrator can delegate the administrator's privilege to other users by including them into the **Admins** built-in group. Please select the **Security→Account** menu. Select **Admins*** in the **Local User/Group** window and click **Property**. Specify the users to have the privilege and click **Apply**.

Chapter 4 Network Configuration

This chapter details concepts and procedures for configuring the NAS system and establishing the system that can communicate among various OS platforms. Management protocol and email notification setting are also covered in this chapter.

4.1 Network Information

The **Network Information** screen is the summary of the current network settings of the NAS system. It provides the administrator a quick look of the basic network setting of the NAS system.

The **Information** page is divided into two sections. The **Network Protocols** section displays the current network protocol settings of the server.

Protocol Type	Display network protocol supported by the server
Configuration	Current status of the network protocol. Status: Enabled or Disabled
Security Policy	Display type of the security policy of the network protocol

The **TCP/IP Suite Settings** section shows the various TCP/IP settings of the server.

Port	Display Ethernet port #.
IP Address	An identifier for a network resource on a TCP/IP network.
Subnet Mask	A subnet mask used to

	determine what subnet an IP address belongs to.
Gateway	A node on a network that work as a point of entry to another network
Speed/Mode	10/100/1000 Mbps and full/half Duplex
Network Teaming Mode	Display the current network teaming mode.
Obtain TCP/IP settings from	Display the IP settings is either assigned automatically from DHCP or assigned manually
WINS Server IP Address	Windows Internet Naming Service (WINS), manages the association of network resources name and its IP addresses without the user or an administrator having to be involved in each configuration change.
DNS Server IP Address	IP address of the domain name system (DNS) server which located the domain names and translate it into IP addresses.
DNS Suffix	Display the DNS suffix
NTP Time Server IP Address	The IP address of the NTP (Network Time Protocol) server, which is used to synchronize system time automatically over the net. The system time will be synchronized with the NTP server every 24 hours.
SMTP Server Address	IP address or server name of the SMTP (Simple Mail Transfer Protocol) server used in sending and receiving e-mail.
HTTP Proxy Server IP Address	IP address of the HTTP proxy server. Next to the IP address is the port number.

4.2 TCP/IP Settings

TCP/IP handles network communications between network nodes that are connected to the network. It is important to setting up correct TCP/IP setting that for NAS system to function properly.

Network Teaming Mode

The NAS system provides two on-board 10/100 or Gigabit Ethernet ports (LAN1 & LAN2). You can configure the Ethernet ports using the following operating modes:

Stand Alone: Each LAN1 & LAN2 are configured with a unique IP address, which are independent to each other.

Fault Tolerance: Uses LAN2 to take over for the LAN1 if LAN1 is fail to connect to the network which designed to ensure server availability to the network.

Load Balancing: Offers increased network bandwidth by allowing transmission to multiple destination addresses using both LAN1 and LAN2. If the traffic of one of the LAN port starts to get congested, requests are then forwarded to the other LAN port with more capacity until the traffic of both LAN ports start to get balance. Note that only the LAN1 Ethernet port receives incoming traffic. **Load Balancing** also incorporates Fault Tolerance protection.

Link Aggregation: combines both LAN1 & LAN2 into a single channel, appearing to use a single MAC address to provide greater bandwidth. It must be used with a network switch having the **Link Aggregation** or **Trunking** function.

Wake-On-LAN

NAS system also supports **Wake-On-LAN** (available for LAN1 only). **Wake-On-LAN** allows administrators to remotely power

on your NAS system to perform maintenance task on the server with no need to go to the server physically.

Jumbo Frame Support

The NAS server can support jumbo frames on Gigabit Ethernet ports, using packet sizes to 9K bytes instead of the standard Ethernet's 1500 bytes. Using the jumbo frames, the NAS server reduces the networking overhead and would hence increase network throughput. In addition to enabling the jumbo frame support on the NAS server, you must also enable the support on the Gigabit switches and client PCs so that they can communicate using jumbo frames.

Configuring TCP/IP Settings

1. Select a **Network Teaming Mode** from the pull-down menu that suit you need.
2. Enable or Disable **Wake On LAN (Available for LAN1 only)**.
3. Click the **Obtain IP settings automatically** radio button to obtain IP addresses of your NAS system from DHCP, BOOTP or RARP server on the network.
4. Or, click the **Use the following IP settings** radio button to assign the IP addresses manually.
5. Note that LAN3 IP address field will appear only when the optional Gigabit Ethernet adapter is installed in your system.
6. Input the **WINS server IP address**.
7. Input the **DNS server IP address**.
8. Input the **DNS Suffix**.
9. Input the **NTP Time Server IP Address** if available.
10. Click **Apply** to save the setting.

To disable a LAN port, enter 0.0.0.0 in its **IP address** field. If you happen to disable all LAN ports and cannot access the administration page, please use the LCD panel to change the IP address to non-zero values.

4.3 Windows Settings

NAS system using SMB/CIFS protocol- short for Server Message Block/Common Internet File System, a protocol used by Microsoft to share files, directories and devices with the Windows client.

You can configure the Windows Network Settings using the following operating mode:

Workgroup Mode: NAS system becomes a member of a workgroup and communicates with the clients using its internal user database for authentication and do not require other authentication server present in the network.

Domain Mode: NAS system become member of a domain and communicates with the client using the user database stored in an authentication server which must be present in the network

Optionally, you can register the NAS system to the domain. Once registered, the NAS system will be created as a machine account on the domain controller. And it will use Netlogon as the authentication mechanism, which provides better integration into the Windows network environment.

Configuring Windows Network Settings

1. Click the **Enable Windows Network (SMB/CIFS Protocol)** checkbox to enable access for SMB client.
2. Enter the Workgroup/Domain name.
3. Click the **Workgroup Mode** radio button if you want to configure NAS system in **Workgroup Mode**.
4. Or, click the **Domain Mode** radio button if you want to configure NAS system in **Domain Mode**.
5. Select the option to support Unicode.
6. Select the option to disconnect idle connection automatically. Server will disconnect the connections

which have been idle for 5 minutes if this option is enabled.

7. Click **Apply** to save the setting.

4.4 UNIX/Linux Settings

NAS system can export shares to UNIX/Linux client via NFS protocol. UNIX/Linux client then can mount the shares and gain access to the content of the shares.

UNIX/Linux client uses UNIX user identification, typically consisting of User Identifier (UID) and Group Identifier (GID), for access control. Non-NFS clients do not use UIDs and GIDs for identification. Since NAS system is intended for working in a heterogeneous network, files created by non-NFS client could possess incorrect ownership information and generate inaccurate quota information for UNIX/Linux clients due to the unmatched UID and GID. A mapping is needed to maintain the correct identity of the user using multiple protocols to access NAS system, for example Windows and UNIX/Linux clients. Windows based clients need to map the Windows user name to UID/GID before forwarding a request to retain the correct ownership information for UNIX/Linux clients.

By default, the NAS system maps all non-NFS users, including local users and domain users, with the same UID/GID as defined on this page. If the administrator wants to have different UID/GID for different users, he should click the **Modify** button to modify the user mapping to UID/GID.

UID: User ID. The numerical number assigned to a user in Unix/Linux permissions. NFS uses UID to determine permissions on files and directories.

GID: Group ID. A part of POSIX permissions that determine groups of users. NFS files have a GID assigned to them.

Permission: Three numbers are used for setting the file permission. Each of the three numbers corresponds to the type of users- Owner, Members of a group and Everyone Else.

Number	Read (R)	Write (W)	Execute (X)
0	No	No	No
1	No	No	Yes
2	No	Yes	No
3	No	Yes	Yes
4	Yes	No	No
5	Yes	No	Yes
6	Yes	Yes	No
7	Yes	Yes	Yes

Example: If the permission of a file is set to 777, this file has read, write and execute permissions for the owner, the group and for other users.

Configuring UNIX/Linux Network Settings

1. Click the **Enable UNIX/Linux Network (NFS Protocol)** checkbox to enable access for NFS client.
2. Enter the default permission for files created via non-NFS protocol. (Default setting = 755)
3. Click **Apply** to save the settings.
4. Click the Modify icon and enter the default UID and GID. (Default setting = 0)
5. Choose to map all users to the default UID/GID or assign UID/GID for each user manually.
6. Click **Set Default** link to set the UID/GID of all users to the default UID/GID. Note that the value '-1' represent that the UID/GID is equal to the default UID/GID configured above.
Or,
7. Click **Apply** to save the settings

Configuring NIS settings

The NIS (network information services), formerly known as Yellow Pages, is a UNIX standard for centralizing the management of UNIX resources. The NAS system supports the retrieval of user accounts and their UID/GID from a NIS server.

If the NIS support is enabled, the NAS system can auto-map NIS users with local/domain users. It matches user names and assigns the UID/GID of the matched NIS users to local/domain users. The user auto-mapping function provides better and tighter integration between NFS clients and other network operating systems.

The steps of enabling NIS support are as follows:

1. Check the **Enable NIS Support** checkbox.
2. The NIS domain name is required. Please fill in the correct name in **NIS Domain Name** field.
3. If you do not know the IP address of the NIS server, please specify **Find by broadcast**. Otherwise, specify the IP address in the fields.
4. After enabling the NIS support, you can auto-mapping NIS users with local/domain users. In **UNIX/Linux** menu, click the **Modify** icon.
5. Click the **Auto-map with NIS users** link to map with the users in the configured NIS server.
6. Click **Apply** to save the settings.

4.5 Macintosh Settings

NAS system supports two kinds of protocols used for Mac OS clients – **AppleTalk** and **TCP/IP (Open Transport)**. Also, NAS system provides two kinds of security policies for Macintosh Network AFP client.

Local account authentication: Authenticate user using NAS system's internal user database.

Local and domain authentication: If **Windows Network** is enabled, you can enable both local and domain authentication for AFP client.

Current Zone: A division between groups of machines when viewed using AppleTalk. AppleTalk Zones can be seen in the Chooser, the AppleTalk Control Panel, and the Network Browser.

AppleTalk Address: It is a unique number that identify the server on the network. The number to the left of the dot is the network number. The number to the right of the dot is the node number.

Configuring Macintosh Network Settings

1. Click the **Enable Macintosh Network (AFP Protocol)** checkbox to enable access for AFP client.
2. Select a protocol and click the radio button beside it.
3. Click the **Local account authentication** radio button to authenticate user using the server's local user database.
4. Or, click the **Local and domain account authentication** radio button to use both local account and Microsoft domain security authentication.
5. Select the **Current Zone** from the pull down menu or **Default Zone** is assigned by default.
6. Click **Apply** to save the setting.

4.6 NetWare Network Settings

NAS system operates in a manner similar to a Novell NetWare 3.12 file server. Setting up your NAS system and shared among Novell NetWare clients. A share can be mapped to the NAS system using NetWare clients. You can enable specific local users or local groups to have access to the share from within the Administration Homepage.

Server Name: The default NetWare server name is the server name followed by an underscore and followed by "NW".

Security Policy: The policy that the NAS system used for authentication.

Frame: Frame types determine how packets of network data are formatted on different LANs. The default setting is AUTO in the NAS system.

Internal Network Number: A logical network number that identifies an individual NetWare server on the LAN.

Configuring NetWare Settings

1. Click the **Enable NetWare Network (NCP Protocol)** checkbox to enable access for NetWare client.
2. The NetWare server name is the original server name following by a "_NW". For example, if the server name of the NAS system is "ABC" then the NetWare server name will be "ABC_NW".
3. Click **Apply** to save the setting.

4.7 Web Data Access Settings

This section shows the parameters that you can set up for user to access NAS system user's home page. You can configure the user access constraint, authentication policy and default setting by defining the **Access Control**, **Security Policy** and **Default User Page** settings.

Configuring Web Data Access

1. Click the **Enable Web Data Access (HTTP Protocol)** checkbox to enable Web data accessing.
2. Choose **Allow file download only** or **Allow file upload and download**.
3. Click the **Local account authentication** radio button to authenticate user using the server's local user database.
4. Or, click the **Local and domain account authentication** radio button to use both local account and Microsoft domain security authentication.
5. Select the default type of the folder display on the user page. You can choose from **Detail View**, **Large Icons** or **Small Icons**.
6. Click the checkbox beside the **Allow users to modify ACL** to give users the privilege to modify the ACL table entries.
7. Click **Apply** to save the setting.

4.8 FTP Data Access Settings

NAS system supports File Transfer Protocol (FTP) that allows users to transfer files via the Internet. By properly configuring the FTP settings, you can effectively control how users access the content in your NAS system via FTP.

Configuring FTP Data Access

1. Click the **Enable FTP Data Access** checkbox to enable FTP data accessing.
2. Select the **Access Control** type. Click the **Allow file download only** or **Allow file upload and download** radio button.
3. Select the appropriate **Security Policy**. Check the **Allow anonymous login and map to:** check-box, and select a local user from the pull down menu. User using the anonymous login will then possess the same security privilege as the selected local user.
4. Or, click **Allow individual user login**. Select **Local account authentication** to authenticate user using the local user database or click the **Local and domain account authentication** radio button to use both local account and Microsoft domain security authentication.
5. Select the **User Limit**. Click the **Unlimited** radio button or specify the maximum number of users allowed to access the content in your NAS system via FTP.
6. Specify the **Home Directory** when user connects to the NAS system via FTP. Note that you must select a volume to create a FTP home directory.
7. Specify the permission of the home directory by clicking the **Set** icon.
8. Click **Apply** to save the setting.

4.9 SNMP Settings

Simple network management protocol (SNMP) provides the ability to monitor and gives status information of the SNMP agent to the SNMP management console. NAS system behaves as an SNMP agent that answers requests from management console and sends trap information to it.

The following options should be configured to using SNMP protocol:

Community: A name serves as a simple authentication. The communication between the SNMP management console and the NAS system cannot be established if the community names are mismatch.

IP: IP address of the SNMP management console

Trap: A trap is a voluntary message send out from a SNMP agent (which is in this case your NAS system) when there is an event occurred.

Management: Configure the SNMP management console as **Read Only** or **Full Control**.

Location: Provide location information of the SNMP agent.

Contact: Provide name of the contact person who has the management information of the SNMP agent.

Configuring SNMP Settings

1. Click the **Enable SNMP Protocol** checkbox to enable SNMP accessing.
2. Enter a **Community** name.
3. Enter the **IP** address of the management console.

4. Select **Yes** from the pull down menu if you want the corresponding management console to receive trap message.
5. Select **Read Only** from the pull down menu if you want the corresponding management console has read only privilege.
6. Repeat Step 2 to Step 5 if more than one management console is available. NAS system supports up to 4 management consoles.
7. Enter the location information of your NAS system.
8. Enter the name of the contact person who has the management information of the NAS system.
9. You can check the checkbox beside **Send a test trap** to send sample trap information to validate your setting of the SNMP settings.
10. Click **Apply** to save the setting.

4.10 Email Settings

You can configure email notification to notify you when there is an event occurred to the NAS system. Enter the information of the SMTP server on your network in this menu; you can configure what kind of event should trigger the email notification process in the **Event→Configuration→Advance** menu.

Configuring Email Settings

1. Click the **Enable SMTP Protocol** checkbox to enable SMTP protocol.
2. Enter the **SMTP Server Address**.
3. Enter an existing user account name of the SMTP server.
4. Enter the password of the account.
5. Enter up to two email addresses you want to send email notification to when event occurred.
6. Click the **Send a test email** checkbox if you want to send out a test email to validate your email setting.
7. Click **Apply** to save the setting.

4.11 SSL Settings

The NAS system enables secure web access by supporting SSL 3.0, both for the user homepage and the administration homepage. To use SSL 3.0, the NAS system will generate a server certificate for authentication and data encryption. By default, the server certificate is issued to the NAS system designated by its IP address. You can also specify to use the server's full name on the server certificate. The server's full name is the server name appended with its DNS suffix, such as **nas.company.com**. Please refer to the TCP/IP settings for DNS suffix.

For clients to access server web-pages with secure connection, they have to install the CA certificate first. Suppose that the server's IP address is 192.168.1.10, please open <http://192.168.1.10/admin/CA> for the certificate. Choose to install the certificate when a dialog-box pops up. Once the CA certificate is installed, the client can access all NAS systems' web pages with SSL connection.

Suppose that the server IP address is 192.168.1.10. To access the NAS system's web pages with SSL connection, please open <https://192.168.1.10/> for the user homepage, or <https://192.168.1.10/admin/> for the administration homepage. If the server certificate with the server name is chosen, please open [https://\[server name\]](https://[server name]) instead.

This page is left blank intentionally

Chapter 5 Storage Management

This chapter describes how to create a single-disk volume or a RAID volume. It also outlines the steps of deleting a volume, expanding a RAID-5 volume and assigning hot-spare disks. After a volume is created, please refer to the next chapter for more information about sharing data and assigning permissions.

5.1 Volume Usage and Status

A volume is a logical storage unit. Each volume holds a complete file-system. A volume can exist on a single disk or a RAID group consisting of two or more disks.

Volume View

List of Volumes

It displays all the volumes in the NAS system. **Volume Name** shows the volume name which is defined when creating a volume. Each volume name is also a hyperlink. It opens a page for showing the detailed information of that volume. **Members** indicate the hard disks which compose the volume. **RAID Type** indicates whether this volume is JBOD (a single hard disk), RAID 0, RAID 1 or RAID 5. Please refer to the next section for more information about RAID.

Free Space indicates the volume usage by showing the free storage space in the volume and the percentage. **Total Space** indicates the volume size.

Status indicates the disk activity on the volume. The disk activity may be one of the following:

Ready	The volume is mounted and ready for data access.
Not Ready	The volume is not mounted successfully. It is not accessible.
Degraded	One of the volume members is defective. Data are still intact and accessible, but the volume is no longer protected by RAID. Data backup and RAID rebuilding are strongly suggested when a volume is in this state.
Faulty	Two or more hard disks in the volume are not functional. It is not possible to perform any data access or recover any data.
Faulty (RW)	Two or more volume members are defective. There might be data loss, but it is possible to recover some data. Please copy data to a safe place immediately when a volume is in this state.
Inaccessible	Two or more volume members are missing. The volume is not mounted and data cannot be accessed.
Apply (Ready) Apply (Degraded) Apply (Faulty RW) Apply (Rebuild) Apply (Expand)	The volume settings on the server and those on the hard disks are inconsistent. It means that the server has to read and apply the volume settings from the hard disks. After the volume settings are restored, it will return to the last known state, which is specified in parentheses.
Checking	Checking the file-system.
Mounting	Mounting the volume for data access.
Create (xx%)	Creating a volume. The progress is shown in percentage.

Rebuild (xx%)	Rebuilding a RAID. The progress is shown in percentage.
Expand (xx%)	Expanding a RAID. The progress is shown in percentage.
Scan (xx%)	Scanning hard disks for bad sectors. The progress is shown in percentage.

Hot-Spare Disks

A hot-spare disk will be used to rebuild a RAID automatically whenever a RAID volume is degraded because of a bad or missing hard disk.

Free disks

These hard disks are not used yet. They can be used to create volumes or assigned as hot-spare disks.

Volume Details and Renaming a Volume

To change the name of a volume, click its **Volume Name** hyperlink in the **List of Volumes** table. It brings to another page for displaying detailed information of the volume. You can modify the volume name on that page.

Device View

It is a list of all the storage devices connected with the NAS system, including hard disks, CD/DVD-ROM, CD/DVD writers and tape drives.

List of hard disks

In Volume shows to which volume the hard disk belongs. **Location** indicates the IDE channel and master/slave position of the hard disk. **Model Name** shows the model or the manufacturer of the hard disk. **Capacity** shows the unformatted capacity of the hard disk. **Status** indicates the disk status or disk activity, being one of the following.

On-line	The hard disk is a member of a mounted volume which is ready for data access.
No init	The hard disk is not initialized yet. A no-init disk must be a free disk, which can be used to create a volume or be assigned as a hot-spare disk.
Defective	The hard disk contains bad sectors.
Off-line	The hard disk is not mounted and not accessible.

Backup/Archiving Devices

These are either CD/DVD-ROM drives, CD/DVD writers or tape drives. **Type** indicates what kind of device it is. **Mode** indicates the data transfer mode of the storage device interface.

Device type could be CD-ROM, CD-R, CD-RW, DVD-ROM, DVD+R, DVD+RW, DVD-ROM+CD-RW or Tape.

Data Transfer Modes

Data transfer modes could be PIO x, DMA x, MDMA x, or UDMA x. PIO means Programmed Input/Output, of which data transfers are performed by host CPU. DMA means Direct Memory Access, of which data transfers are done by device controllers and use little host CPU time. MDMA is multi-word DMA. UDMA is Ultra DMA, which is a faster DMA mode.

PIO Modes	PIO Mode 2: 8.3 Mbytes/sec PIO Mode 3: 11.1 Mbytes/sec PIO Mode 4: 16.6 Mbytes/sec
DMA Modes	Multiword DMA Mode 2: 16.6Mbytes/sec Ultra DMA Mode 2: 33 Mbytes/sec Ultra DMA Mode 3: 44 Mbytes/sec Ultra DMA Mode 4: 66 Mbytes/sec Ultra DMA Mode 5: 100 Mbytes/sec Ultra DMA Mode 6: 133 Mbytes/sec

5.2 Creating a Volume

The first thing for the administrator to do with the storage is to create a volume on the hard disks. Then he or she can share the storage for user access and set security control.

To create a volume, first go to the **Volume→Create** page. Specify the volume name in the **Volume Name** field and choose the volume type (JBOD, RAID 0, 1 or 5). Then choose the hard disks to be included in the volume. Last, click **Apply** to submit changes. The progress of volume creation is shown on the **Volume→Information** page.

Below are the volume types.

JBOD	Just a Bunch Of Disks. A JBOD-type volume contains only one hard disk as its member.
RAID 0	RAID level 0 is disk striping only, which distribute data evenly over multiple disks for better performance. It does not provide safeguards against failure. RAID level 0 uses two or more hard disks.
RAID 1	RAID level 1 uses disk mirroring, which provides 100% duplication of data. It offers high reliability, but doubles storage cost. RAID level 1 uses two hard disks.
RAID 5	RAID level 5 distributes data and parity bits over multiple disks for both performance and fault tolerance. A RAID volume can still work when a hard disk fails. RAID level 5 uses three or more hard disks. Building a RAID-5 volume may take hours depending on capacity.

5.3 Deleting a Volume

To delete a volume, go to the **Volume→Delete** page. Select the volume to be deleted and click the **Delete** button. Please be very careful because all data in the volume will be destroyed and the RAID configuration will be erased also. All hard disk members in this volume will become free disks after the deletion.

5.4 Expanding a RAID-5 Volume

RAID-5 volume expansion makes it possible to enlarge volume capacity without rebooting the NAS system. Volume capacity grows on the fly. Moreover, you do not have to change any share permissions, security controls and quota settings after volume expansion. Storage management becomes much easier.

To expand a RAID-5 volume, please go to the **Volume→Expand** page. Select a RAID-5 volume to be expanded. Then choose the free disks as new members. Click **Apply** to submit changes. The progress of RAID expansion is shown on the **Volume→Information** page.

To expand a SmartExtend volume, please open the administration page of the SmartExtend target system. When the target volume is connected to the initiator, use the **Volume→Expand** function to expand the target volume.

5.5 SmartExtend – Add More NAS Capacity

The SmartExtend feature can add NAS capacity over LAN. A SmartExtend initiator can connect up to 10 SmartExtend target volumes via the Giga- or Fast-Ethernet ports. A target volume can provide up to 2TB of capacity, so it can increase NAS capacity by as much as 20TB!

Please note that the SmartExtend initiator is an optional feature on model 4200/4400/4420/8200/8400/8420.

The following table explains some terms used by SmartExtend.

SmartExtend Initiator	A NAS head. It can add more capacity by connecting with SmartExtend target volumes over network. A SmartExtend initiator can connect to 10 SmartExtend target volumes at most.
SmartExtend Target	A system which contains target volumes. Target volumes are used to add capacity to a SmartExtend initiator.
SmartExtend Target Volumes	JBOD or RAID groups on a SmartExtend target system.
SmartExtend Network-Attached Devices	Once connected, SmartExtend target volumes appear as free disks on a SmartExtend initiator system. Different from a locally-attached hard disk, a SmartExtend device is network-attached.
Exported SmartExtend Target Volumes	Target volumes must be exported to network first before being seen and used by SmartExtend initiators.
Group Allowed/Login User	The use of a SmartExtend target volume is restricted to the SmartExtend initiator and the user group which are assigned when it is exported. Only the specified SmartExtend initiator can use the

	target volume. And the initiator must provide a user account for authentication when it tries to connect to the target volume.
Connected/ Disconnected	Indicates the status of a SmartExtend target volume. If connected, a SmartExtend initiator can access data in the SmartExtend target volume. A SmartExtend initiator will try to connect to every target volume in the target volume list when it starts up.
Automatic Recovery of Broken Connections	If network is not very stable, a SmartExtend target volume might be disconnected occasionally. A SmartExtend initiator will try to recover a broken connection every 5 minute. The feature improves data availability even in a poor network.

Configuring SmartExtend Step By Step

At least two NAS systems are required, one as an initiator, another as a target. SmartExtend initiators provide all NAS file-sharing functions, acting as NAS heads connecting to SmartExtend targets. SmartExtend targets are network-attached RAID systems for SmartExtend. They have no NAS functions.

Model 4200/8200 or above can become SmartExtend initiators. This function is an optional feature which must be activated by a license key. Please contact the vendor to obtain the license key.

All models can become SmartExtend targets. You do not have to activate the function.

Follow the steps below to build a SmartExtend connection between an initiator and a target.

- on the SmartExtend initiator system

1. After getting the license key, go to the **Server*License** page to enter the license key and activate the feature.
2. Go to the **Server→General** page. Change the SmartExtend mode to **NAS with SmartExtend Initiator**.

- on the SmartExtend target system

3. Go to the **Server→General** page, change the SmartExtend mode to **SmartExtend Target**.
4. Go to the **Volume→Create** page, create a JBOD or RAID volume. It is suggested to create hot-spare disks after you create a RAID-1 or RAID-5 volume.
5. Check the **Volume→Information** page and make sure that the volume is created successfully.
6. Go to the **Volume→SmartExtend** page. Export the target volume by clicking the **Export Volume** button.
 - (a) First specify the target volume to be exported.
 - (b) Specify the group who can use the target volume. A SmartExtend initiator must provide a user account when it tries to use the target volume. The user account must be a member of this group.
 - (c) Specify a SmartExtend initiator which will connect to this target volume.
 - (d) Apply the settings.
7. On the **Volume→SmartExtend** page, you will see the target volume in the list, but the Status column will show **Disconnected**. You will need to build the connection from the SmartExtend initiator side.

- on the SmartExtend initiator system

8. Go to the **Volume→SmartExtend** page, click the **Add** button.
 - (a) Choose the SmartExtend target system from the SmartExtend Target List or specify the IP address manually. Click the **Next** button.

- (b) On the page, it will list all the target volumes found on the SmartExtend target system. Choose the target volume to connect to.
 - (c) Specify the username and password for authentication. It must be a member of the group specified in Step 6.(b)
 - (d) Click the **Finish** button.
9. On the **Volume→SmartExtend** page, you will see the target volume listed in the table. It will need about 10-30 seconds to build the connection, depending on network traffic. Click the **Refresh** hyperlink to refresh the page. The device name should be SED01, standing for **SmartExtend Device number 01**.
10. Go to the **Volume→Information** page, check if SED01 is in the **Free Disks** list. If yes, it means that it is not initialized yet. Go to the **Volume→Create** page to initialize it.

Now you are done. Repeat the above steps until all SmartExtend volumes are created ok.

Expanding a SmartExtend RAID-5 Volume

To expand a SmartExtend volume, please open the administration page of the SmartExtend target system. When the target volume is connected to the initiator, use the **Volume→Expand** function to expand the target volume.

5.6 Volume/Disk Scan

Volume/Disk scan is especially useful for disk diagnostics and repairs lost or cross linked clusters in Volume/Disk. All readable data will be placed in new clusters and defective cluster will mark as bad in the file system. All the newly added devices will be scanned before usage to ensure the data integrity in the NAS Server.

Select the volumes or disks you want to scan, click **Scan Now** button to start scanning. Or, click **Schedule** to set the time for NAS Server to perform scanning at the scheduled time.

Disk Auto-scanning

To make sure that the hard disks contain no bad sectors before putting into use, it is suggested to perform disk-scanning before taking such actions as creating a volume, expanding a volume, migrating data or assigning a hot-spare disks. If disk auto-scanning is enabled, the NAS server can scan disks automatically when you perform these actions. If the hard disks have ever been scanned in the last 30 days, the auto-scanning will be skipped so that the auto-scanning will not be activated too often.

To enable the feature, please click the **Configure** hyperlink on the **Volume→Scan** page. Set the **Disk Auto-scanning** item to **Enabled**.

5.7 Assigning Hot-spare Disks

The hot-spare disks are global, which means they are not bound to any specific RAID volumes. Whenever a RAID volume goes degraded because of a bad hard disk, a hot-spare disk will be taken immediately to recover that RAID volume.

To assign hot-spare disks, please go to the **Volume→Create** page. Specify the volume type as Hot-spare. Assign the free disks as hot-spares by using the dual window panes. Click **Apply** to submit changes.

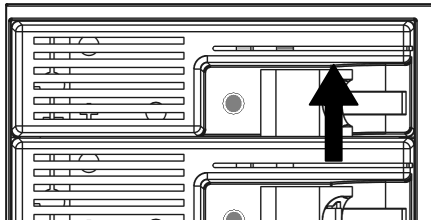
To remove disks from the hot-spare list, please go to the **Volume→Delete** page. Select the hot-spares to be deleted in the **Remove Hot-Spare Disks** table and click **Delete**.

5.8 Hot-swapping

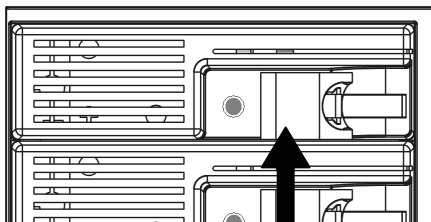
You may have to change hard disks in some situations, such as hard disk failure, degraded RAID or general maintenance. The NAS system supports HDD hot-swapping if used with MR-423I hot-swappable HDD module. Below are the instructions of replacing hard disks when using the HDD module.

When using MR-423I hot-swappable HDD module:

1. Identify which hard disk fails. The amber LED of the HDD tray will blink to indicate hard disk failure.



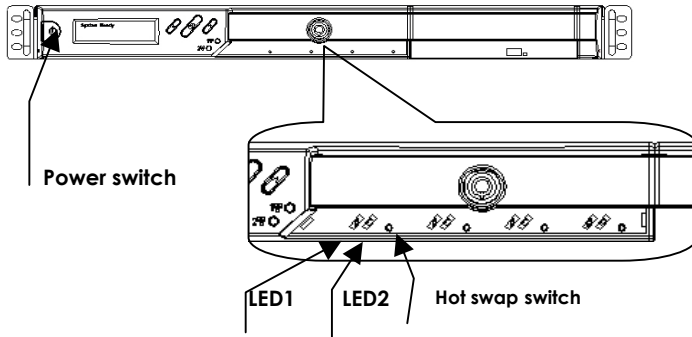
2. Turn off the failed HDD by pressing the red button on the HDD tray.



3. When the amber LED is steady on, it is ready for being unplugged. Unplug the HDD tray and replace the HDD with a good one.
4. Plug in the HDD tray. Wait until the Green LED is steady on. Then you are done.

When a RAID volume is degraded and there is no available hot-spare disk for rebuilding, the RAID volume will stay in the degraded state. In this state, you can hot-unplug the failed hard disk and plug in a good one in the same HDD tray. The RAID volume will rebuild automatically with the new hard disk.

For 1U rack mount model (4100R & 4200R):



1. Identify which hard disk fails. The amber LED2 will blink to indicate hard disk failure.
2. Turn off the failed HDD by inserting the end of a large straightened paper clip into the hot swap switch hole on the front bezel.
3. When the amber LED is steady on, the failed HDD is ready for being unplugged. Unplug the HDD tray and replace the HDD with a good one.

Plug in the HDD tray. Wait until the Green LED is steady on. Then you are done.

This page is left blank intentionally

Chapter 6 Security Control

This chapter covers how to setting up the security control of the files, folders and shares stored in NAS system. Managing Access Control List (ACL) file level security, file ownership and user quota are also covered in this chapter.

You can configure the following types of security control on the NAS system:

1. Create, edit and delete user accounts in the local user database.
2. Create shares.
3. Configure Files, Folders and shares permission.
4. Configure local account, domain account and UNIX/Linux Hosts permission.
5. Maintain the ACL table.
6. Configure the local user and domain user quota limit.

6.1 Security Information

The **Security Information** screen is the statistic of the current security setting of the NAS system. It provides administrator a summary of the security database and the status of the operation mode.

The **Information** page is divided into two sections. The Security Database section display the number of shares, number of ACL nodes and number of user/group.

Number of Shares	Total number of share created in NAS system.
Number of ACL Nodes	Total number of ACL node created. ACL tells NAS system which access right each user has to a folder or an individual file.
Number of	The total account number of the

Accounts	Local User/Group, Domain User/Group, Trust Domain User/Group and Unix/Linux Host Entry.
Local User/Group	Total number of local user/group. A local user or group is an account that can be granted permissions and rights from NAS system.
Domain User/Group	Total number of domain user/group. Domain users or groups are managed by the network administrator.
Trust Domain User/Group	Total number of trust domain user/group.
Host Entry	Total number of Unix/Linux host entered.

The **Security Configuration** section shows the current security configuration settings of the server.

Windows Security Mode	Display the status of the Windows Network operating mode. Status: Domain Mode or Workgroup Mode
Workgroup/Domain Name	Display either the workgroup name or domain name
Domain Login Account	Display the username for retrieving the domain user list in the domain.
ACL Security Control	Display the status of the ACL Security Control. Status: Enabled or Disabled
User Quota Control	Display the status of the User Quota Control. Status: Enabled or Disabled

6.2 Creating the Local User and Local Group Accounts

A local user or group is an account that can be granted permissions and rights from your NAS system. You can add local user to a local group. Groups are indicated by a * sign at the suffix of the name. You can also grant administrator privilege to a local group. Groups with administrator privilege are indicated by a # sign at the suffix of the name.

To create a local user:

1. Go to **Security→Account→Local Account** menu.
2. Click the **Add User** button.
3. Type in the user name and enter the password.
4. Re-type the password to confirm.
5. Click **Apply** to save the setting.

To create a local group:


-
1. Go to **Security→Account→Local Account** menu.
 2. Click the **Add Group** button.
 3. Type in the group name.
 4. If you want to grant the administrator privilege to this group, click the **Grand administrator privilege** check box.
 5. Select the users from the left hand windows and click the **>>** button to join the group.
 6. Click **Apply** to save the setting.




Note:

If you want to grant administrator privilege to a user, simply add the user to the built-in group **Admins** which has administrator privilege. User with administrator privilege can access the administration home page.

View and change local user property:

1. Go to **Security→Account→Local Account** menu.
2. Select a user.
3. Click the **Property** button.
4. If you want to change the password, enter a new password and confirm.
5. If you want to disable this user account, click the **Disable user account** checkbox.
6. Select a group from the left hand window and click the  button to add the user as a member of this group in the **Member of** section.
7. Click **Apply** to save the setting.

View and change local group property:

1. Go to **Security→Account→Local Account** menu.
2. Select a group.
3. Click the **Property** button.
4. If you want to grant the administrator privilege to this group, click the **Grand administrator privilege** checkbox.
5. You can see all the members of this group in the right hand window.
6. Select a user from the left hand window and click the  button to add this user to the group.
7. Click **Apply** to save the setting.

6.3 Caching Windows Domain User Accounts

Domain users and groups are managed by your network administrator. Windows network use a domain controller to store the information of all the domain users and groups. When the **Windows Network** is set to using **Domain Mode** in your NAS system, you need to cache domain account in the NAS system's local user database. By caching domain accounts, it speeds up the process of setting permissions and quotas.

To retrieve Windows domain user/group:

1. Go to **Security→Account** menu.
2. Click the **Domain Account** tab.
3. If you have not entered the valid **Domain Login Account** for retrieving Windows domain users and groups, click the **Modify** button. Otherwise, go to Step 7.
4. Enter a **User Name** and **User Password** of an existing account of the domain which shown in the **Domain Name** field.
5. Click **Apply** to save the setting.
7. You can change to another domain from the pull down menu which has the trust relationship with the current domain to retrieve domain users and groups.
8. Select the domain users or groups from the left hand windows and click the **>>** button to join the authorized list which will be stored at the local user database.
9. Click **Apply** to save the setting.



Note:

If you modify the domain name or change the Windows security mode (Workgroup or Domain), all the domain users and groups in the NAS system user database will be cleared.

Synchronize user database

This function synchronizes the domain accounts cached in the NAS user database with the native domain controller. New domain accounts in the domain controller will be added to the NAS user database, while the non-existent domain accounts will be removed from the NAS user database. Due to the limitation of system resource, the user database synchronization will be skipped if there are more than 10,240 domain accounts in the domain controller.

To synchronize with the domain controller, please click the 'Synchronize user database' hyperlink. You can also set up the NAS server to synchronize the NAS user database automatically by checking the option - **Synchronize the user database with the native domain automatically**. The synchronization interval is one hour.

Update user database

Changes of user accounts on the domain controller will not affect the NAS system automatically. You have to do it manually. The '**Update user database**' function on the **Domain Account** tab of the **Security→Account** menu helps you find the user accounts which have already been deleted from the domain controller, yet still remain in the NAS user database. You can choose to delete them from the database. ACL and share permission will be also updated by removing the entries related to those users.

6.4 Creating UNIX/Linux Host

For NAS system, NFS client's mount privileges are granted specifically to UNIX/Linux host created by the administrator. If a UNIX/Linux host is granted access right to a share in the NAS system, user of the UNIX/Linux host can have access to the share. Administrator should create a UNIX/Linux host list prior to grant access right to them.

To create a list of the UNIX/Linux host:

1. Go to **Security→Account** menu.
2. Click the **UNIX/Linux Host** tab.
3. Enters a single host IP address in the first text box.
4. Or, enter the start IP address in the first text box and the last 3 digits of the end IP address in the second text box to input a range of the host IP addresses of the **Host IP** field.
5. Click the **Add** button to add the host IPs to the host list.
6. Click **Apply** to save the setting.



6.5 Creating Share and Assigning Share Permissions

You can share a specific folder in any volume created in the NAS system with others on the network. When you create a share, you can assign the permission to the share that other users will be allowed or denied when they access the share over the network.

To create a new share:

1. Go to **Security→File/Folder** menu.
2. Locate the volume you want to share on the volume lists.
3. Click the **Create** hyperlink to share the corresponding volume. Then go to Step 9.
4. If you want to share an existing folder under a volume, click the volume name hyperlink. Click the folder hyperlink until you reach the desire directory. Then, go to Step 8.
5. If you want to share a new folder under a volume, click the folder hyperlink until you reach the desire directory path.
6. Click the **Create Folder** button to create a new folder.
7. Enter a new folder name and click **Apply**.
8. Click the **Create** hyperlink to share the corresponding folder.
9. Enter a unique share name in the **Share Name** field. The share name is what user will see when they connect to this share. The actual name of the folder does not change.
10. To add a comment about the share, type the text in **Comment**.
11. To limit the number of users who can connect to the share, on the **User limit**, click **Allow** and enter a number of users.
12. Select the protocols you want to share.
13. Click **Apply** to save the setting.

To assign share permission of a share for local account and domain account:

1. Go to **Security→Share** menu.
2. Locate the share and click  to assign or modify share permission to this share.
3. Highlight the users or groups from the left hand windows.
4. Select the appropriate permission from the pull down menu at the bottom of the left hand windows.
5. Click the  button to join the privileged list.
6. You can modify the permission of the users or groups in the privileged list by first highlight the users or groups and then select the appropriate permission from the pull down menu at the bottom of the right hand windows.
7. Click **Apply** to save the setting.

**Note:**

You can also modify share permission in **Security→File/Folder** menu by click the **Modify** hyperlink of the corresponding shared folder.

You can assign the following share permission to a user on NAS system:




No Access (NA) – Account has been denied access to the share.

Read Only (RO)– Account is allowed to read the share.

Read Write (RW)– Account is allowed to read and write to the share.

Full Control (FC) – Account is allowed to read both read and write and change permission to the file or folder.

To assign share permission of a share for UNIX/Linux Host:

1. Go to **Security→Share** menu.
2. Locate the share and click  to assign share permission to this share.
3. Click the **UNIX/Linux Host** tab.
4. Assign the UID, GID and Permission of this share. It will overwrite the ownership and permission of the mount point once the share is mounted by the NFS client. If the NIS support is enabled, the UID and GID pull-down menus will list all NIS users for you to choose.
5. You can allow all hosts to access the share with read/write or read only permission. Then go to Step 9.
6. Or, you can specify privileged hosts by highlight the host IP from the left hand windows.
7. Select the appropriate permission from the pull down menu at the bottom of the left hand windows.
8. Assign which UID/GID the root account of the UNIX host should be converted into when accessing the share. This is the 'root squash' function.
9. Click the  button to join the privileged list.
10. You can modify the permission of the hosts in the privileged list by first highlight the privileged host and then select the appropriate permission from the pull down menu at the bottom of the right hand windows.
11. Click **Apply** to save the setting.
12. If you want to remove shares, check the corresponding checkbox located at the end of the row and click .

You can assign the following share permission to UNIX/Linux Hosts on NAS system:

Read Only (RO) – the host is allowed to read the share.

Read Write (RW) – the host is allowed to read and write to the share.

6.6 Configuring File and Folder Security and ACL

Access Control Lists (**ACL**) are associated with each file and folder, as well as the list of users and groups permitted to use that file or folder. When a user is granted access to the file or folder, an ACL node is created and added to the ACL for the file or folder.

If you assign permissions to a local user, a Security ID (SID) created by NAS system will be referred by the ACL for the file and folder security. If the local user is then deleted, and the same name is created as the previous one, the new user does not have permissions to the file or folder, because the SID will not be the same. The administrator will have to re-configure all the group memberships and access rights to the files and folders.

Since the Security ID (SID) for domain user is issued and maintain by the domain controller on the network. Administrator do not need to re-configure all the group memberships and access rights to the files and folders if the domain user is deleted from the local user database and the same name is created as the previous one.



Note:



If the administrator changes the permission on a file or folder that a user is currently accessing, the permission setting do not take immediate effect because of the local handle being used by the user. The new rights will only take effect when the user reconnects to the file or folder.

There are two built-in user accounts: **Admin** and **Guest**. And two built-in group accounts: **Admins** and **Everyone**. Every user of NAS system including local and Domain user is the member of the **Everyone** group. By default, when a volume is

created, **Admins** and **Admin** will be granted Full Control permission and **Everyone** will be granted Read/Write permission to the volume.

After you set permissions on a volume, all the new files and folders created under the volume inherit these permissions. If you do not want them to inherit permissions, uncheck the **Inherit from parent folder** when you set up the permissions for the files and folder.

Configuring file and folder security:

1. By default, **ACL control** is enabled.
2. Go to **Security→File/Folder** menu.
3. Locate the file or folder you want to configure the permission.
4. Click the  icon. If the icon is disabled, go to **Security→ACL** menu to enable the **ACL Control**.
5. Clear the **Inherit from parent folder** check box.
6. Select the users or groups from the left hand windows and click the  button to join the privileged user/group list.
7. If you want all the subfolders and files inherit the new permission you have just set, check the **Propagate to all subfolders and files** check box.
8. Click **Apply** to save the setting.

You can assign the following File/Folder permission to a user on NAS system:

No Access (NA) – Account has been denied access to the file or folder.

Read Only (RO) – Account is allowed to read the file or folder

Write Only (WO) – Account is allowed to write to the file or folder

Read Write (RW) – Account is allowed to read and write to the file or folder.

Full Control (FC) – Account is allowed to read both read and write and change permission to the file or folder.

Set file/folder permission in Windows Network

NAS system provides a simple, efficient way to set up and maintain file/folder security in Windows Network. To change permissions, you must have been granted permission to do so by the administrator. Below is the permission mapping table of NAS system in Windows Network:

File/Folder Permission in NAS system	Folder Permission in Windows Network	File Permission in Windows Network
No Access (NA)	<input type="checkbox"/> Full Control <input type="checkbox"/> Modify <input type="checkbox"/> Read & Execute <input type="checkbox"/> List Folder Contents <input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> Full Control <input type="checkbox"/> Modify <input type="checkbox"/> Read & Execute <input type="checkbox"/> Read <input type="checkbox"/> Write
Read Only (RO)	<input type="checkbox"/> Full Control <input type="checkbox"/> Modify <input checked="" type="checkbox"/> Read & Execute <input checked="" type="checkbox"/> List Folder Contents <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> Full Control <input type="checkbox"/> Modify <input type="checkbox"/> Read & Execute <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Write Only (WO)	<input type="checkbox"/> Full Control <input type="checkbox"/> Modify <input type="checkbox"/> Read & Execute <input type="checkbox"/> List Folder Contents <input type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input type="checkbox"/> Full Control <input type="checkbox"/> Modify <input type="checkbox"/> Read & Execute <input type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Read/Write (RW)	<input type="checkbox"/> Full Control <input checked="" type="checkbox"/> Modify <input checked="" type="checkbox"/> Read & Execute <input checked="" type="checkbox"/> List Folder Contents <input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input type="checkbox"/> Full Control <input type="checkbox"/> Modify <input type="checkbox"/> Read & Execute <input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Full Control (FC)	<input checked="" type="checkbox"/> Full Control <input checked="" type="checkbox"/> Modify <input checked="" type="checkbox"/> Read & Execute <input checked="" type="checkbox"/> List Folder Contents <input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Full Control <input checked="" type="checkbox"/> Modify <input checked="" type="checkbox"/> Read & Execute <input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write

To set, view, change or remove file/folder permission in Windows Network:

1. Locate the file or folder you want to set permission

2. Right-click the file or folder, click **Properties → Security**
3. Change permission from an existing groups or users, click the **Allow** or **Deny** checkbox
4. Or, remove the groups or users by clicking the **Remove** button.

To change owner of a file or folder


1. Go to **Security→File/Folder** menu.
2. If you want to change the owner's name of the corresponding file and folder, click the owner's name hyperlink. Select a new owner from the user list.
3. Check the checkbox beside **Apply to all sub folders and files** if you want to propagate the ownership to all sub folders and files.
4. Click **Apply** to save the setting.

6.7 Managing Quotas

Configuring user quota:

NAS system supports two types of quotas: user quota and folder quota. User quota monitors the disk space usage of each user. It is based on file ownership, and is independent to which volume that the file and folder located. Below are the descriptions of the parameters when setting up user quotas.

User Name	User name in the local user database.
UID	The user ID set in the user mapping table in Network → UNIX/Linux menu.
GID	The group ID set in the user mapping table in Network → UNIX/Linux menu.
Type	User type. Local or Domain .
In Use	Total amount of disk space used by the user.
Quota Limit	The amount of disk space in MB a user is allowed to use.

1. Click the **Enable user quota control** checkbox to enable user quotas.
2. Enter quota limit in MB for the user under the **Quota Limit** column.
3. You can click the  **Recalculate** to obtain the most updated information of the total amount of disk space used by each user.
4. Click **Apply** to save the setting.


To set all quotas to the same value, please specify the quota value in the **Set all quotas to xx MB** input field. Click the **Set** hyperlink to save settings.




Configuring folder quota:

Folder quota monitors the amount of data that can be stored on the folder on which folder quota is applied regardless of who saves there. It can limit the total amount of data stored in

Managing Quotas

the NAS system to effectively control the proper consumption of the storage resources. Note that it is prohibited to set folder quota to the Volume root or "System folder" and its sub-folders.

Folder Name	The path and folder name that the folder quota has been applied.
In Use	Total amount of disk space used.
Quota Limit	The amount of data that can be stored in the respective folders.
	Delete quota entries by selecting the check box at the end of each quota entries and click this icon.

1. Click the **Enable folder quota control** checkbox to enable folder quotas.
2. Click the  **Add** to add folder quota to a folder.
3. Click the  **Select Path** to browse for target folder.
4. Enter the quota limit in MB.
5. Click **Apply** to save the settings.
6. You can click the  **Recalculate** to obtain the most updated information of the total amount of disk space in use on each folder.

To set all quotas to the same value, please specify the quota value in the **Set all quotas to xx MB** input field. Click the **Set** hyperlink to save settings.

This page is left blank intentionally

Chapter 7 Disc Sharing and Data Archiving

Disc Server creates and manages CD and DVD disc images for easy and fast disc sharing. It relieves the efforts of handling huge amount of discs. Thousands of discs can be kept online for user access. To protect those disc images, all NAS servers are equipped with a robust RAID sub-system, which features hot-spare disks and strong data protection.

7.1 Start to Use the Disc Server Function

The Disc Server function is activated on model 4100/8100 by default. It is an optional feature on model 4200/4400/4420/8200/8400/8420. To active the function on these models, please get a license key from your vendor and enter the key on the **Server→License** menu of the administration page.

At least 256MB memory is required for the Disc Server function to work. The NAS server can manage more disc images with more memory.

It requires some simple configuration before using the Disc Server function. Please open the administration page, select **Quick Setup** from the **Disc Server** menu. On the page, select the CD or DVD device which will duplicate the disc image automatically when a disc is inserted. Then specify the folder to store the duplicated disc images. Click **Apply** to save the settings.

Insert a disc into the CD or DVD device. It should start duplicating the disc image immediately. When it finishes, network users can access the disc by opening the MIRROR share of the NAS server.

7.2 Creating Disc Images

Using the local optical device to duplicate disc images

The simplest and fastest way to create a disc image is to use the CD or DVD device of NAS server to duplicate the inserted discs. Usually a CD can be duplicated in 5 to 10 minutes.

To configure a device so that it can automatically duplicate any inserted discs, please go to the **Disc Server→Disc Caching** menu page of the administration page. In the **Device List** table, click the hyperlink text in the CD Device's **Function** column and change the CD function to **Disc Mirroring**.

The Disc Mirroring Settings section will appear on the page. Select a folder as the target location. The folder is called **Disc Image Folder**, which is a folder especially for storing disc images. In addition to create a new disc image, it can also replace an existing disc image with the duplicated one. If the disc image being replaced is shared, the duplicated disc image will inherit all the share settings and permissions. The CD replacement will happen once and it will return to the previous settings.

The disc image's name can be either inherited from the CD label or user-defined. A user-defined name will only apply once to the next duplicated disc image.

Copying disc images via network filing protocols or SmartSync

The disc images are stored in the disc image folders. Administrators can also copy or sync the disc images from one NAS to another, using Windows Explorer, MacOS Finder or SmartSync.

When disc images are copied to a disc image folder, the NAS server will not recognize them immediately. Administrators must

command the NAS server to discover disc images manually or set up the NAS server to discover disc image regularly.

To discover disc images manually, please open the **Disc Server→Disc Images** administration page and click the **Re-scan images** hyperlink to the right of the page.

To set up the NAS to discover disc images regularly, please open the **Disc Server→Information** page. Configure the **Disc Server Settings** to enable the NAS server to scan for disc images every one hour.

Using the remote mirroring software to create disc images

Please refer to Appendix B - Utility for NAS system for how to use the remote mirroring software.

7.3 Managing Discs

Once the disc image is created in the NAS server, it can be seen on the **Disc Server→All Disc Images** menu of the administration page.

If the disc images are not created or duplicated by the NAS server or by the remote mirroring software, administrators will have to re-scan the disc image folders for disc images manually. For example, if disc images are copied from another NAS server to a disc image folder over network using the Windows or other OS platforms, the NAS server will not be able to list them on the **Disc Images** page. In such cases, administrators have to click the **Re-scan images** hyperlink text to the right of the page.

To change the disc name:

To change the disc name, click on the hyperlink text in the **Disc Name** column. On the same page, it also shows detailed information of the disc image.

To delete a disc image:

To delete a disc image, check the check-boxes to the right and click the **Delete** icon.

7.4 Sharing Discs

Administrators can choose to share a single disc, multiple discs or a disc image folder. If a single disc is shared, its content will be shown when users open the network share. If multiple discs are shared, the discs will appear as individual folders under the network share. The folder names are the same as the disc names. If a disc image folder is shared, all the discs in the disc image folder will appear as individual folders under the network share.

To share a single disc:

To share a single disc, go to the **Disc Server→Disc Images** menu of the administration page. Click the **Create** hyperlink in the **Share** column. Click **Apply** to share the disc. Enter the **Share Permissions** tab to assign user permissions if you want to restrict user access. The **Unix/Linux Setting** tab is for configuring NFS security settings. Please refer to section 6.5 - 6.5 Creating Share and Assigning Share Permissions for the details of share permissions and NFS security settings.

You can also go to the **Disc Server→Disc Shares** page to share a single disc. Click the **Create Disc Share** button. Specify the share name and click **Apply** to create the share. Select the disc to share in the **Share Target** tab and click **Apply**.

To share multiple discs:

To share multiple discs, go to the **Disc Server→Disc Shares** page. Click the **Create Group Share** button. Specify the share name and click **Apply** to save settings. Select the discs to share in the **Share Target** tab and click **Apply**. Use the **Share Permissions** tab or the **Unix/Linux Setting** tab if you want to restrict user access.

To share a disc image folder:

To share a disc image folder, go to the **Disc Server→Disc Images→Disc Image Folder** menu of the administration page. Click the **Create** hyperlink in the **Share** column. Specify the share name and click **Apply**. Use the **Share Permissions** tab or the **Unix/Linux Setting** tab if you want to restrict user access.

You can also go to the **Disc Server→Disc Shares** page to share a disc image folder. Click the **Create Disc Folder Share** button. Specify the share name and click **Apply** to create the share. Select the disc image folder to share in the **Share Target** tab and click **Apply**.

7.5 Burning Disc Images

To burn an existing disc image, select **Disc Recording** from the **Disc Server** menu on the administration page. To do disc recording, the CD function must be configured as **Loader/Writer**. To change the CD function, please click the hyperlink in the **Function** column of the **Device List** table.

Next, select a disc image by clicking the **Select a Disc** hyperlink. After the selection is made, the disc image information will be shown underneath, including image size, disc format and disc volume label. Check the **Erase disc before writing** option if it is a rewriteable disc which contains data. Click **Apply** to start the disc recording.

7.6 Archiving Data to CD/DVD Discs

Data archiving is to move or copy NAS data to CD/DVD discs regularly. Administrators can set file filters, mostly based on file date/time, to specify what to burn. One of the applications is to move obsolete data out of the NAS server so that disk space can be freed for future uses.

If used with the Disc Server function, the Data Archiving function becomes more versatile. You can choose to turn some less-frequently-used files to read-only disc images first, which can be mounted by the Disc Server function to share to network users in read-only forms. When the archived data are not in use for long, you can then choose to burn them to discs, freeing the hard disk space.

The Archive Folder

During data archiving, the NAS server will first create disc images in the **archive folder**, which is a disc image folder specifically for storing archived data in the form of disc images. Please firstly specify the location of the archive folder on the **Disc Server→Data Archiving→Summary** page before you use the data archiving function.

Summary Logs

On the **Disc Server→Data Archiving→Summary** page also shows the summary logs, which keep track of the execution summary of the data archiving tasks.

In addition, they keep records like which disc images are created, which are burned and which are not burned. Click the **View** hyperlink under the **Discs** column of the **Summary Logs** table to view the list of disc images. For those disc images not burnt yet, you can choose to burn them.

Setting Up Data Archiving Tasks

On the **Disc Server→Data Archiving→Tasks** page, you can create tasks to archive data manually or on schedules.

Task Name	Specifies the name of the data archiving task, for management purpose
Source Folders	Specify the data to be archived. The folders, not preserving the full paths, will be archived to CD/DVD discs
Disc Label	Specifies the labels of the CD/DVD discs.
Date Extension	If the date extension is enabled, it will append the date of archiving to the disc labels. For example, ARCH20041010_01 is the first disc created by the data archiving task on October 10, 2004 with the date extension. The second disc will be ARCH20041010_02 if more than one disc are created.
Disc Type	Specifies the media for burning. It can be CD, DVD or dual-layer DVD. The NAS server will create disc images that match the size of the disc type, and then burn the disc images.
Advanced Settings – File Filtering	<p>At first the settings are hidden. Please click the Show hyperlink to display the advanced settings.</p> <p>The file filters specify which files in the source folders to include for data archiving. You can choose to include only the files which are in the specified date range. Or, you can choose to include the files which are N days old. Or, you can choose to include only the files of which the archive bits are set. (The NAS server</p>

	will clear the archive bits of the source files which are archived, if not deleted.)
Advanced Settings – Skip Archiving (Do Archiving only if...)	<p>You can set constraints so that the archiving task is activated only when one of the following conditions is met.</p> <p>if the free volume space is lower than n% – in other words, the data archiving will be skipped if the free volume space is high</p> <p>if the archived data are over n MB/GB – that is to say, the data archiving will be skipped if the archived data are below the threshold</p>
Archiving Schedule	Specifies the schedule of the archiving task. If the schedule is due, the NAS server will check if the conditions specified in the Advanced Settings are met. If met, perform the data archiving task.
Options	<p>Delete source files after the archiving is completed – if checked, the NAS server will delete the source files to free up disk space after data are successfully archived in disc images or burned to discs.</p> <p>Burn Disc – if checked, it will archive data to CD or DVD discs. Multiple CD/DVD writers can be specified here. Please note that the CD functions must be set to Loader/Writer before putting into use for burning.</p>

Chapter 8 User Access

The NAS system fits into the network environment as soon as it is properly configured. This chapter describes how to get the NAS system ready for user access from various network OS.

Before reading on, please make sure that the NAS system is configured with an IP address and a volume is created successfully. For the rest of the sections, we assume that the server name is **NASSERVER**, the IP address is **192.168.170.172** and there is a volume named **volume01**.

8.1 Workgroup or Domain Mode

The NAS system can work in either the workgroup mode or the domain mode. In the workgroup mode, the administrator creates accounts for the NAS system and maintains the user database per server. User authentication is done by checking the local user accounts. In the domain mode, the NAS system can retrieve user names from the domain controller and rely on the domain controller to authenticate users. It can also authenticate users by local accounts.

In the domain mode, when a Windows user requests to access a shared folder, the user will be authenticated with the local accounts first, then the domain accounts. If the user is assigned with proper access rights in the share permissions and the ACL settings, the user will be allowed to access the shared folder.

For those using MacOS, web browsers or FTP to access the NAS system, the security control mechanism is similar. If set to the workgroup mode, the NAS system authenticates all users from various network operating systems with local accounts only. If set to the domain mode, the NAS system can be configured to use different security policies for different network file protocols – either authenticated by local accounts only, or by both local and domain accounts.

For example, the NAS system can authenticate Windows users by querying the domain controller, while at the same time check the MacOS users with local user accounts. The administrator can set the SMB/CIFS protocol to the domain mode and configure the AFP protocol to apply **Local account authentication**.

8.2 Accessing from Windows

There are some configuration jobs to do before Windows users can access the NAS system. Please enter the administration homepage first.

1. Please configure the NAS system to operate either in the workgroup mode or the domain mode.
Go to the **Network→Windows** menu and select either **Workgroup Mode** or **Domain Mode**. Also specify the workgroup/domain name. It will require a server reboot afterwards.
2. Create local accounts if the NAS system is in the workgroup mode.
Go to the **Security→Account→Local Account** page and use the **Add User** or **Add Group** button to create local accounts.
3. Get domain accounts from the domain controller if the NAS system is in the domain mode.
Go to the **Security→Account→Domain Account** page. Then click the **Modify** button and give a domain user account for logging on to the domain controller to retrieve domain accounts. Next, use the and buttons to specify the domain accounts to be cached in the NAS system.
4. Share the volume to network users.
Go to the **Security→File/Folder** menu. Find the **volume01** entry and click **Create** in the **Sharing** column (or click **Modify** if the volume has been shared). On the **Property** page, check the **Windows Network (SMB/CIFS)** checkbox and click **Apply**.
5. Set the share permissions.
After sharing the volume, specify the access rights of local users/groups and domain users/groups.

Now Windows users can access the NAS system. They can run the Windows Explorer and open the path of [\\nasserver](#). The shared folder **volume01** will appear in the window.

Windows users can also map a network drive to [\\nasserver\volume01](#) or use the **net use** command in the **Command Prompt** window. The command will be like:

```
net use n: \\nasserver\volume01
```

8.3 Accessing from Web Browsers

In addition to the administration homepage, the NAS system provides the user homepage for normal users to access data in the server. With a web browser, users can download files, create folders, upload files and modify ACL.

To enable user access from web, please follow the steps.

1. Enable the user homepage.
Open the administration page and enter the **Network→Web** menu. Check the **Enable Web Data Access** check-box. Specify whether to allow local accounts only or allow both local and domain accounts to access the user page. Check other parameters and click **Apply**.
2. Create local user accounts or retrieve domain accounts from the domain controller, depending on whether the NAS system is in the workgroup mode or the domain mode.
3. Share the volume to network users.
Go to the **Security→File/Folder** menu. Find the **volume01** entry and click **Create** in the **Sharing** column (or click **Modify** if the volume has been shared). On the **Property** page, check the **Web Access (HTTP)** check-box and click **Apply**.
4. Set the share permissions.
After sharing the volume, click the **Share Permissions** tab to specify the access rights of local users/groups and domain users/groups.

Now users can run the web browser and open the IP address of 192.168.170.172 to browse the NAS system. When the user homepage is opened, it prompts for user name and password. Then it will display all shared folder after user login. The user homepage will be like:



In the top right corner of the user page are the tool-bar icons, which provide access to various functions like creating folder or uploading files. Below the tool-bar are the server name and the login user. Lower on the page is a file browsing area.

Tool-bar icons



Admin Page: switches to the administration home page.



Change View Mode: changes the views of the file browsing area between **Detail**, **Large Icons** and **Small Icons**.



Change Password: modifies the password of the login user. It allows a local user to change the password.



Create Folder: creates a new folder in the current path if the login user has the access right.




Upload File: uploads files to the current path if the login user has the access right.





Help: opens a new browser window with help information

File Browsing

When the user page is opened, the file-browsing window shows all the shares in the server. All the folders and files are presented as hyperlinks. If a folder is clicked, it will show its content in the same window. When a file is clicked, it will either open the file in another browser window or pop up a dialog-box for download. To move to the upper level of directory, click the  Up Directory icon.

To delete files or folders, check the checkboxes in the **Delete** column. And click the **Delete** icon  to delete them.

If a user has the **Full Control** access right for a file or folder, he can modify its ACL by clicking the ACL icon  in the  Permission column.

8.4 Accessing from MacOS

After setting the NAS system to operate in the workgroup mode or the domain mode, follow the steps below to configure for MacOS user access.

1. Enable the Macintosh Network support (the AFP protocol).
Open the administration page and enter the **Network→Macintosh** menu. Check the **Enable Macintosh Network** check-box and specify the security policy and the AppleTalk zone. Then click **Apply**. In the workgroup mode you can only select **Local account authentication** as the security policy. In the domain mode, you can select either one.
2. Create local user accounts or retrieve domain accounts from the domain controller, depending on whether the NAS system is in the workgroup mode or the domain mode.
3. Share the volume to network users.
Go to the **Security→File/Folder** menu. Find the **volume01** entry and click **Create** in the **Sharing** column (or click **Modify** if the volume has been shared). On the **Property** page, check the **Macintosh Network (AFP)** check-box and click **Apply**.
4. Set the share permissions.
After sharing the volume, specify the access rights of local users/groups and domain users/groups.

After the configuration is done, MacOS 8 or OS 9 users can use the MacOS **Chooser** or **Network Browser** to access the NAS system. Mac OS X users can use the **Connect to Server** function to open the NAS system.

For example, open the **Connect to Server** window in **Finder**.



You can either type the IP address of **NASServer** in the **Address** field. And click **Connect** to put it on **Desktop**. Or you can click **AppleTalk** in the middle left window pane to find the zone and the server. Once you find the server, click **Connect** to put it on **Desktop**.

8.5 Accessing from FTP Clients

You can set an FTP home directory in the NAS system for user access. Login authentication is done by checking the ACL of the FTP home directory. During an FTP session, the server always checks ACL when it receives any FTP requests, such as `ls`, `put`, `get`, etc. Local accounts and domain accounts are both supported, depending on the security policy.

After setting the NAS system to operate in the workgroup mode or the domain mode, follow the steps below to configure for FTP access.

1. Enable the FTP Data Access feature.
Open the administration page and enter the **Network→FTP** menu. Check the **Enable FTP Data Access** check-box and specify the security policy. In the workgroup mode you can only select **Local account authentication** as the security policy. In the domain mode, you can select either one. Then specify the FTP home directory as **volume01** and click **Apply** to save the settings.
2. Create local user accounts or retrieve domain accounts from the domain controller, depending on whether the NAS system is in the workgroup mode or the domain mode.
3. Configure the folder security settings of **volume01** to control user access.
Click the **Set** hyperlink to specify the access rights (ACL) for the FTP home directory – **volume01**. These will be the accounts which are allowed to login the NAS using ftp software. Note that the **Inherited List** will be cleared if you uncheck the **Inherit from parent folder** check-box and click **Apply** button.

Now, run an FTP client to connect to `192.168.170.172`. Login as the user you assign in step 3 above. Then you will be able to access **volume01**.

8.6 Accessing from NFS Clients

The security control of the NAS system for NFS clients follows the traditional UNIX-style trust-host mechanism and UID/GID checking. Follow the steps below to enable NFS support and export the volume for NFS clients to mount.

1. Enable the UNIX/Linux Network support (the NFS protocol).
Open the administration page and enter the **Network→UNIX/Linux** menu. Check the **Enable UNIX/Linux Network** check-box and click **Apply**.
2. Go to the **Security→Account→UNIX/Linux Host** page and add the hosts that might be trusted to access the NAS system.
3. Export the volume to NFS clients.
Go to the **Security→File/Folder** menu. Find the **volume01** entry and click **Create** in the **Sharing** column (or **Modify** if the volume has been shared). On the **Property** page, check the **UNIX/Linux Network (NFS)** check-box and click **Apply**.
4. Enter the **UNIX/Linux Setting** tab. Add NFS clients to the privileged host list. And assign UID, GID and permission octets to the exported volume.

After the volume is exported, use one of the NFS clients in the privileged host list to mount the volume. Please login as the root and use the following command to mount **volume01** under the **/mnt** directory.

```
mount 192.168.170.172:/volume01 /mnt
```

Once mounted, the **/mnt** directory will link to **volume01** and inherit the same UID, GID and permission as you specify in the configuration steps. The users on the NFS client with proper access rights will be able to access the **/mnt** directory and hence the NAS system.

This page is left blank intentionally

Chapter 9 Backup and Recovery

9.1 Snapshot – Fast Point-In-Time Copies

Snapshots are read-only copies of file-systems at a specific point in time. Snapshot distinguishes itself in its speed. Creating a snapshot is not involved with copying user data, thus usually taking less than a second.

The concept of snapshot is very different from tape backups. Data are not copied to any media during backup. Instead, it just informs the NAS that all the data blocks in use should be preserved, not being overwritten. That is why it can be so fast. The “copy” occurs during everyday file access. When a file is modified after a snapshot is created, its original data blocks are protected from being overwritten. The new updates are written to a new location. The file-system maintains records and pointers to keep track of the snapshot data and file changes.

The snapshot feature is activated by default on model 4400/4420/8400/8420. It is an optional feature on model 4100/4200/8100/8200.

Snapshot Management

To manage snapshots, please open the administration page. Enter the **Backup→Snapshot→Manage** page and select a volume.

Viewing Snapshot Information

On the page shows the snapshots existing on the volume and their information. **Snapshot Used Space** indicates the disk space used by snapshot data. In the table – **List of Snapshots**, **Space to Free** indicates the disk space which will be freed if a

snapshot is deleted. **Activity** indicates whether the snapshot is being deleted or rolled back.

Configuring Snapshot Settings

Show the .snap folder	With the .snap folders enabled, end-users can access snapshot data without intervention of MIS people, retrieving previous versions of files from the .snap folders. Administrators can choose to show the .snap folders under the root of a volume, or under all folders.
Name the .snap folder as ~snap	Using the AFP protocol, the folders with names beginning with dot (.) will be hidden and not able to be accessed by Macintosh clients. To make the .snap folders visible, the administrators can choose to show the .snap folders as ~snap instead so that the folders can be accessed by Macintosh clients.
Delete snapshots if free space is low	If enabled, it will automatically delete the oldest snapshots to free more disk space when the free space is lower than the specified percentage.
Snapshot Policy	They specify how many hourly, daily, weekly and monthly snapshots to keep, respectively. If the limit is exceeded, the oldest snapshot of the same type will be deleted. If not specified, it will keep the snapshots until being manually deleted.

Creating Snapshots Manually

To manually create a snapshot, please click the **Create Snapshot** button on the bottom of the **Snapshot→Manage** menu page. It will create a snapshot with a name like manual-

20041010.190000, which indicates a snapshot created manually at 19:00:00 of October 10, 2004.

Deleting Snapshots

To delete snapshots, check the check-boxes in the **List of Snapshots** table and click the **Delete** icon to delete the selected snapshots. You can make multiple selections to delete several snapshots at a time. The NAS server will delete the snapshots one by one.

Snapshot Roll-back

Snapshot roll-back is to restore the volume to the state when the selected snapshot was taken. Snapshot roll-back is useful if most data are lost or destroyed by virus attacks or human errors. Snapshot roll-back is much faster than restoring from tapes. Please note that the roll-back operation is dangerous because the whole volume will be restored to the previous state. If you want to restore only part of the data, please simply copy them from the .snap folders to the current file-system.

Snapshot Scheduling

To manage snapshot schedules, please open the administration page. Enter the **Backup→Snapshot→Schedule** page.

To add a snapshot schedule, either click the **Add Schedule** icons next to the volume names, or click on the **Add Schedule** button on the bottom of the page.

To delete snapshot schedules, check the check-boxes to the right and click the **Delete** icon.

To modify a snapshot schedule, click the hyperlink of the snapshot schedule in the **Schedule** column.

There are four types of schedules – hourly, daily, weekly and monthly. Each volume can have up to 8 schedules of any types.

9.2 Loading and Writing CD/DVD Discs

Connecting a CD or DVD writer to the NAS system, you will be able to load data from CD/DVD discs or burn files on writeable CD/DVD discs. The CD and DVD burning feature turns the NAS system into a device that publishes data, beyond the powerful data storage function.

Loading CD/DVD Data

The **Loader** function copies data from a CD or DVD disc to any location inside the NAS system. This function is useful when you try to restore the archived data on CD/DVD discs or simply copy files from discs to the server.

Note that the NAS system recognizes only data CD or DVD, such as ISO 9660. Multimedia CD formats such as audio CD or video CD are not supported.

To load data from CD/DVD discs, please insert the source disc into the CD or DVD device first. Open the **Administration Page** and select **Backup→Loader/Writer**. Then follow the steps below.

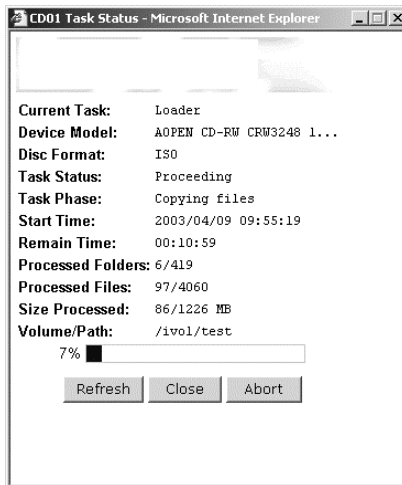
The screenshot shows the 'Loader/Writer' configuration page in the NAS Administration interface. The top navigation bar includes 'Server', 'Network', 'Volume', 'Security', 'Event', 'Status', and 'Backup'. Below this, a sub-navigation bar shows 'Tape Backup', 'SmartSync', 'Loader/Writer', and 'System Profiles'. The 'Loader' tab is selected. The main section is titled 'Copy data from CD or DVD discs' and contains the following configuration options:

- Device List:** A table listing available devices.

Device	Type	Location	Model Name	Mode	Status
CD01	DVD-ROM	CH5, Slave	DVD-ROM DDU220E	MDMA 2	Ready
- Source Device:** A dropdown menu showing 'DVD-ROM DDU220E'.
- Target Path:** A text field containing '/JBOD' and a 'Select Path' button.
- Overwrite Options:** Three radio buttons:
 - ☒ Never overwrite the existing files
 - ☐ Always overwrite the existing files
 - ☐ Overwrite older files with newer files

An 'Apply' button is located at the bottom right of the configuration area.

1. Select a **Source Device** where you insert the disc to be loaded. Above the **Source Device** item you will see a device list for your reference.
2. Specify the destination. Click the **Select Path** hyperlink and select a target path.
3. Choose whether to overwrite the existing files. “**Overwrite with newer files**” means it will overwrite the target if the files on the CD/DVD disc are newer.
4. Click **Apply** to start copying data.



When it is copying disc, you can see the progress by clicking the hyperlink in the **Status** column of the **Device List**. A separate browser window will pop up. The progress is indicated by the progress bar, the **Processed Folders** item, the **Processed Files** item and the **Size Processed** item.

Writing CD/DVD Discs

The NAS system supports CD or DVD burning. It can use ISO-9660 CD format to write data to CD or DVD discs. Supported

Loading and Writing CD/DVD Discs

devices are CD-RW, DVD-RW and DVD+RW writers. Dual-layer DVD writing is also supported.

To write data to CD/DVD discs, please insert a blank disc into the CD/DVD writer first. Next, open the **Administration Page** and enter the **Backup→Loader/Writer** page. Then follow the steps below.

The screenshot shows the 'Writer' tab in the 'Backup→Loader/Writer' menu. The 'Write data to CD or DVD discs' section is active, displaying a device list, target device selection, source folder selection, and various options like disc volume label and overwrite options.

Server | Network | Volume | Security | Event | Status | Backup | Virus Scan |

Tape Backup | SmartSync | **Loader/Writer** | System Profiles |

Loader | **Writer**

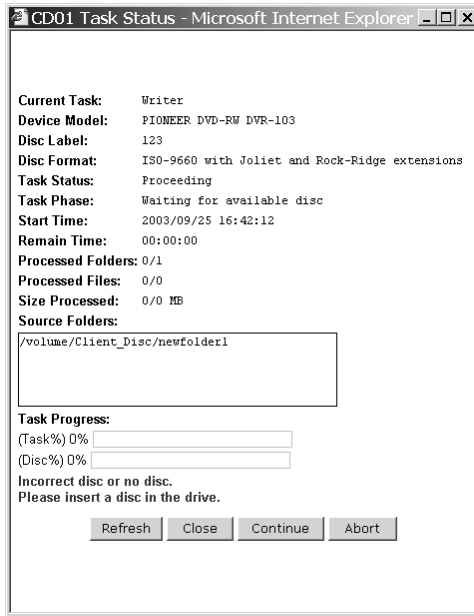
➤ Write data to CD or DVD discs

- Device List

Device	Type	Location	Model Name	Mode	Status
CD01	DVD-RW	CHS,Master	PIONEER DVD-RW DVR-103	MDMA 2	Ready
CD02	CD-RW	CHS,Slave	Hewlett-Packard CD-Writer Plus 9500	UDMA 2	Ready

- Target Device:
- Source Folders:
===== selected folders =====
- Total file size: 0 MB
- Writer Format: ISO-9660 with Joliet and Rock-Ridge extensions
- Disc Volume Label:
- Overwrite Options: ☐ Erase disc before writing

1. Click the **Writer** tab in **Backup→Loader/Writer** menu
2. Select the **Target Device** where you want to burn the blank CD/DVD disc(s). Above the **Target Device** item you will see a device list for your reference.
3. Specify the source folders. Please click **Select Folders** and specify which folders to burn.
4. Specify the volume label of the CD or DVD disc.
5. Check the overwrite option if you want erase a rewriteable disc first before burning.
6. Click **Apply** to start burning CD or DVD discs.



When it is writing to disc, you can see the progress by clicking the hyperlink in the **Status** column of the **Device List**. A separate browser window will pop up. The progress is indicated by the progress bar, the **Processed Folders** item, the **Processed Files** item and the **Size Processed** item. You can also check the **Task Phase** to see what the CD/DVD writer is doing.

If it requires more than one disc to burn the source data, it will prompt for a new disc after the first disc is burned ok. In this case, the **Task %** progress bar indicates the total task progress, which means the percentage of the source data which have been burned to discs. The **Disc %** progress bar indicates the CD/DVD writing percentage of the current disc.

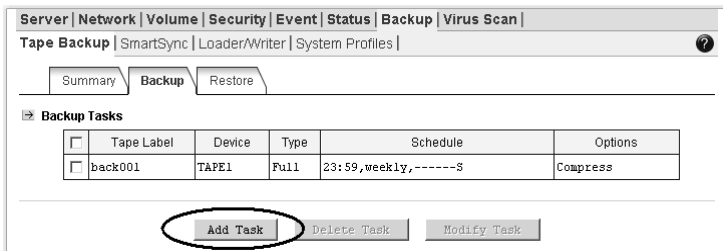
9.3 Tape Backup and Restore

The NAS system builds in backup software for data protection. The backup software features full or incremental backup, scheduled tasks and multi-volume backup. The administrator is able to define backup policy by incorporating one or more backup tasks. It can also utilize the hardware compression capability. It is simple, yet powerful enough to fulfill most backup demands.

The backup software requires the system folder to operate. To specify the system folder, please open the **Administration Page** and go to the **Server→Maintenance** page. Then specify a volume to contain the system folder. If there exists no system folder in the specified volume, it will create one automatically.

Adding Backup Tasks

To arrange backup schedules, please open the **Administration Page** and go to **Backup→Tape Backup** page. Click the **Backup** tab. You will see a list of scheduled tasks on that page.



The screenshot shows the 'Tape Backup' page with tabs for Summary, Backup, and Restore. The 'Backup' tab is active. Below the tabs is a table titled 'Backup Tasks' with columns: Tape Label, Device, Type, Schedule, and Options. There is one task listed: 'back001' on 'TAPE1' with a 'Full' type and a schedule of '23:59,weekly,-----S'. The 'Options' column for this task is 'Compress'. Below the table are three buttons: 'Add Task' (circled), 'Delete Task', and 'Modify Task'.

<input type="checkbox"/>	Tape Label	Device	Type	Schedule	Options
<input type="checkbox"/>	back001	TAPE1	Full	23:59,weekly,-----S	Compress

Add Task **Delete Task** **Modify Task**

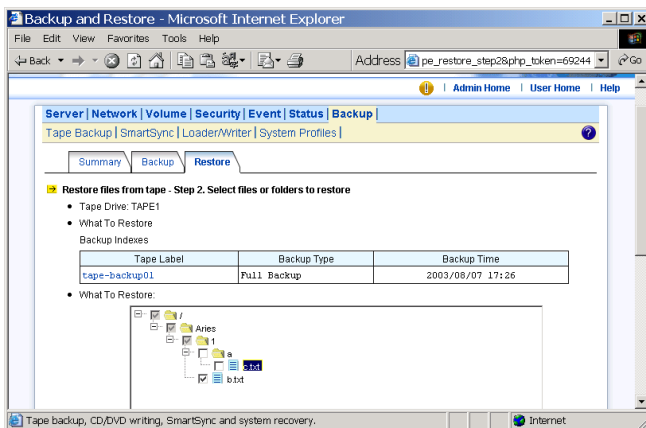
To add a task, click the **Add Task** button. Then follow the steps below.

1. Select a tape drive for backup.
2. Input the tape label for identifying tapes. It will append backup start date/time to the tape label when running a backup task.

3. Specify whether it will be a full or incremental backup task. A full backup task copies all selected folders and files into tapes. An incremental backup task only copies modified or newly created files since last backup. It checks archive bits and only back up those with archive bits set.
4. Choose which folders to back up. Click the **Select Folders** hyperlink and select what to back up. Your selection will be copied to the lower list-box, which indicates the folders to back up.
5. Specify backup schedule. You can start the backup immediately or arrange a schedule. The schedule can be specified at any weekday or a day of a month.
6. Specify whether to overwrite the tape. If yes, the backup task will rewind the tape to the beginning and overwrite it with backup files. If not, it will append the backup to the tape, not overwriting any existing data on tape.
7. Specify whether to enable hardware compression capability when the tape drive has the feature.
8. Click the **Apply** button.

Restoring Files from Tape

To restore data from tape, please open the administration page and go to **Backup→Tape Backup** page. Click the **Restore** tab and follow the steps below.



1. Specify the **Tape Drive** for restoring.
2. Specify a backup set to restore by selecting a backup index. The backup indexes are required to restore data from tape. When the backup indexes are missing, you have to import them from tapes for further restoring operation. To import backup indexes, please select a tape drive and click the **Import** hyperlink.
3. Choose whether to restore all the files in the backup set, or only certain files or folders. For the latter, it requires Java virtual machine for the UI. Please go to <http://java.sun.com> for the latest Java virtual machine.
4. Click the **Next** button.
5. To restore selected files or folders, please make selections on the Java UI in the **What to Restore** item.
6. Choose the target location. It can restore data to either the **original location** or an **alternative location**.
If the original location is selected, it will restore data to the location where they are originally backed up. Please note that if the original volume is missing, it will not restore anything.
The alternative location means any user-defined path. Please use the **Select Path** hyperlink to specify the path. It will restore files and the full directory hierarchy under the specified path.
7. Specify whether to restore the ACL settings together with the files.
8. Specify whether to overwrite the existing files with the backup files.
9. Click the **Apply** button to start to restore.

Checking Task Progress, Viewing Logs

When a tape task is running, you can view its progress on the **Summary** page. On the upper **Summary** page is a list of tape drives. Any task currently running will be shown as a hyperlink in the **Status** column. Click a hyperlink to watch task progress and details. It shows **Ready** without hyperlinks if there is no running task.

Tape Backup and Restore

Server | Network | Volume | Security | Event | Status | Backup | Virus Scan |

Tape Backup | SmartSync | Loader/Writer | System Profiles |

Summary | Backup | Restore

Device List

	Device	Type	Location	Model Name	Mode	Status
	TAPE1	TAPE	CHS_Master	OnStream ADR Series	MWDMA 2	backing up

Rewind

Retention

Erase

Refresh

Summary Logs

Tape Label	Action	Start Time	
back001	Full Backup	2003/06/20 16:09	<input type="checkbox"/>

After a backup or restoring task finishes, it will keep summary logs in the system folder. On the lower **Summary** page are the logs. They keep records of the statistics and errors of the backup/restoring tasks ever executed. Click a hyperlink in the **Tape Label** column to see its details. To delete logs, please check the check-boxes to the right and click the **Delete** icon.

9.4 Using a Tape Library

First, set up the tape library so that it can be controlled by software. Please refer to the tape library's instruction manuals for details. Then, connect the tape library to the NAS server with a SCSI cable. The NAS server supports up to two tape libraries.

The tape library support is an optional feature on model 4200/4400/4420/8200/8400/8420.

Managing Devices, Tapes and Tape Cleaning

When the NAS server starts up, it will initialize the tape library. It might take a while. To view the status, please open the administration page and enter **Backup→Tape Library→Devices**. When it finishes the initialization, you will see a page as below.

The screenshot displays the 'Tape Library' management interface. At the top, there is a navigation bar with tabs: Server, Network, Volume, Security, Disc Server, Backup, Virus Scan, Event, and Status. Below this is a sub-navigation bar with 'Tape Backup' and 'Tape Library' (selected), followed by links for SmartSync, Loader/Writer, and System Profiles. A secondary bar contains buttons for Summary, Devices (selected), Media Pool, Backup, Restore, and Clean.

The main content area is divided into two sections:

Device List

Device	Location	Model Name	Status
LIB1	Host:0,Ch:0,Id:2,Lun:0	SONY LIB-162 0100	Idle
TAPE1	Host:0,Ch:0,Id:0,Lun:0	SONY SDX-500C 010c	Idle
TAPE2	Host:0,Ch:0,Id:1,Lun:0	SONY SDX-500C 010f	Idle

Below the table are buttons for 'Inventory', 'Lock Door', and 'Unlock Door'.

Tape Media on LIB1

Slot # ▲	Tape Label	Bar Code	Media Pool	Status
Slot 01	s1	000058	pool2 (Save Set)	Idle
Slot 02	s2	000007	pool1 (Save Set)	Idle
Slot 03		000059		Idle

At the bottom of the section are buttons for 'Quick Erase', 'Erase', 'Retention', and 'Scan'.

Inserting and removing tape cartridges

The NAS server will initialize the tape library at start-up and lock the door. To insert or remove tapes from the tape library with no cartridge access ports (CAP), please unlock the door first. Then follow the tape library's instruction manuals to insert or remove tapes. Afterwards, lock the door again so that the tape library can resume to work. It will start the inventory process automatically to read in all media information after the door is locked.

For some tape libraries which have cartridge access ports (CAP), use the 'Import/Export' function to insert or remove tapes from the tape library. To insert a tape, first place the tape in the CAP by following the tape library's instruction manual. Use the 'Import' function to move the tape to an empty slot. The NAS server will read the tape and add it to its inventory. To remove a tape, use the 'Export' function to move it to the CAP.

Inventorying tape slots

It checks all the slots of the tape library to see if they are occupied and reads in media information from all the tapes. The whole process may take a while, depending on the number of tapes and the tape drive speed.

Erasing a tape

The quick-erasing function overwrites the tape header only. It takes much less time than erasing a tape, which wipes out all data in the tape. To quick-erase or erase a tape, please click the radio button in front of the slot and click the **Quick Erase** or **Erase** button.

Retensioning a tape

To retension a tape is to wind the tape evenly so that it is properly tensioned. Use this feature only when there are errors accessing the tape. To retension a tape, please click the radio button in front of the slot and click the **Retension** button.

Scanning a tape for backup indexes

If the backup index files are missing, the NAS server will not be able to restore the data. In this case, please insert the tapes and scan them for backup indexes. The NAS server will copy the backup indexes from the tapes. To scan a tape, please click the radio button in front of the slot and click the **Scan** button.

Defining a Media Pool

A media pool is a group of tapes managed as a unit. You must define a media pool before assigning any backup schedules.

To define a media pool, please go to the **Backup→Tape Library→Media Pool** menu and click **New Pool**.

Server | Network | Volume | Security | Disc Server | Backup | Virus Scan | Event | Status |

Tape Backup | Tape Library | SmartSync | Loader/Writer | System Profiles |

Summary | Devices | Media Pool | Backup | Restore | Clean

Please specify the media pool name and the tapes to be added into the media pool. You can also change the tape labels manually. Only blank tapes can be added. To erase a tape, please go to the **Devices** page.

Create a New Media Pool

- Media Pool Name:
- Tape Library:
- Select Tapes:

	Slot Number	Tape Label	Media Type	Bar Code
<input checked="" type="checkbox"/>	Slot 1000	<input type="text" value="sample001"/>		000002

Apply Close

Each media pool is divided into two sets, the save set and the scratch set.

The save set is consisted of the tapes containing important data which cannot be overwritten. On the other hand, the scratch set is consisted of the tapes which are free to be overwritten. At the very beginning, all tapes are empty and locate in the scratch set. When the NAS server backs up data to a tape, the tape is moved to the save set. After the

Using a Tape Library

retention period is passed, the tape expires and is moved to the scratch set for recycling.

The retention period is the number of days for which the tape must be kept in the save set after it is last written. You can define the retention period when creating a backup task.

Backing Up Data

To start a backup task immediately, please go to the **Backup→Tape Library→Backup** menu on the administration page. Click the **Backup Now** button and specify the following.

The screenshot shows a web-based management interface with a top navigation bar containing links: Server, Network, Volume, Security, Disc Server, Backup, Virus Scan, Event, and Status. Below this is a sub-navigation bar with links: Tape Backup, Tape Library, SmartSync, Loader/Writer, and System Profiles. The main content area has tabs: Summary, Devices, Media Pool, Backup, Restore, and Clean. The 'Backup Now' window is open, displaying the following configuration options:

- Task Name: [Text input field]
- Tape Library: LIB1
- Tape Drive: Auto (dropdown menu)
- Backup Media:
 - ☐ Media Pool: [Dropdown menu]
 - ☒ Select Tapes: [Text area containing "There is no available device"]
- Backup Type: Full (dropdown menu)
- What To Back Up: Select Folders (button)
 - [Text area containing "selected folders"]
- Overwrite Options:
 - ☒ Append to the media
 - ☐ Overwrite the media
- Backup Options:
 - ☒ Use hardware compression if available.

At the bottom of the window are 'Apply' and 'Close' buttons.

1. Specify the task name. The created backup set will be named after the task name, appended by date/time.
2. Choose a tape library and the tape drive. Usually the tape drive is set to **Auto**, allowing the NAS server to choose any available tape drive to do the backups.

Using a Tape Library

3. Select backup media. If you have defined any media pool, just select one. If not, you can choose the tapes to use for this backup task.
4. Choose to make full backups or incremental backups. A full backup will copy all source data. An incremental backup will only copy those data with archive bits set. After backup, the archive bits of the source data will be cleared.
5. Specify what to backup by selecting the folders to be backed up.
6. Specify whether to enable the hardware compression capability of the tape drives.
7. Click **Apply** to start to back up.

To create a backup task, please go to the **Backup→Tape Library→Backup** menu on the administration page. Click the **Add Task** button and specify the following parameters.

Server | Network | Volume | Security | Disc Server | **Backup** | Virus Scan | Event | Status |

Tape Backup | **Tape Library** | SmartSync | Loader/Writer | System Profiles |

Summary | Devices | Media Pool | **Backup** | Restore | Clean

Add Task

- Task Name:
- Tape Library: **LIB1** ▼
- What To Back Up: **Select Folders**

===== selected folders =====

- Backup Schedule: **Add a Schedule**

Schedule	Type	Tape Drive	Media Pool	Period	
No schedule					

- Backup Options
 - ☒ Use hardware compression if available.

Apply Close

1. Specify the task name. The created backup set will be named after the task name, appended by date/time.
2. Choose a tape library.
3. Specify what to backup by selecting source folders.
4. Add backup schedules by clicking the **Add a Schedule** hyperlink.

- a) Select the tape drive. Usually it is set to **Auto**, allowing the NAS server to choose any available tape drive to do the backups.
 - b) Select backup media. Please define a media pool on the **Backup→Tape Library→Media Pool** menu if there is no media pool.
 - c) Choose to make full backups or incremental backup. A full backup will copy all selected data. An incremental backup will only copy those data with archive bits set.
 - d) Set schedules.
 - e) Specify the tape retention period. A retention period is the number of days in which you want to keep the backup data from being overwritten. For example, if the retention period is set to 7 days, the tape will remain in the save set as long as it has been used and be moved to the scratch set when it has not been used for 7 days.
 - f) Set overwrite options. If **Overwrite the media** is selected, it will only use blank tape or scratch tape for backups and write data from the beginning of the tapes. If **Append to the media** is selected, it will append data to the last used tape.
5. Specify whether to enable the hardware compression capability of the tape drives.
 6. Click **Apply** to start to back up.

Restoring Data

To restore data, go to the **Backup→Tape Library→Restore** menu. First, select the backup task which created the backup sets. Then select a backup set and specify whether to restore all files or only partial of them. To view the information of the backup set, click the hyperlink in the **Backup Type** column.

Next, choose to restore all files or only certain files or folders. For the latter, you need to install Sun Java virtual machine v1.4 or higher. Please go to <http://java.sun.com> and download the software. Use the Java UI to select the files or folders to be restored.

Next, choose the destination: the original location or alternative location. If the original location is selected, it will restore the files to exactly where they are backed up. If the original volume is missing, it will not restore anything. If the original folders are missing, it will create the folders automatically.

If the alternative location is selected, it will restore data to a user-specified location. The full tree hierarchy of backup data will be reconstructed under that location.

Restore security: when checked, it will restore the access control lists (ACL) together with the data.

Overwrite Options – specify whether to overwrite the existing files with the backed up files.

Checking Task Progress, Viewing Logs

When a task is running, you can view its progress on the **Devices** page. On the upper page is a list of tape libraries and tape drives. Any currently running tasks will be shown as hyperlinks in the **Status** column. Click a hyperlink to watch task progress and details. It shows **Idle** with no hyperlinks if there is no running task.

After a backup or restoring task finishes, it will keep summary logs in the system folder. On the **Summary** page you will see the summary logs. They keep records of the execution summary information of the backup or restoring tasks. Click a hyperlink in the **Task Name** column to see its details. To delete logs, please check the check-boxes to the right and click the **Delete** icon.

9.5 SmartSync – NAS-to-NAS Data Replication

The NAS systems are integrated with the SmartSync function for NAS-to-NAS data replication. Two or more NAS systems are required, one as the SmartSync server, others as the SmartSync clients. The SmartSync server is like an ftp server. The SmartSync clients can either replicate their data to the SmartSync server, or copying data from the SmartSync server, depending on the task settings.

There are three operating modes of SmartSync - "**mirror**" for one-to-one data replication, "**backup**" for disk-based backup, "**distribute**" for one-to-many data distribution. The following sections describe the usage and applications of these operating modes.

The function of creating sync points of backup mode or distribute mode are only available on model 4400/4420/8200/8400/8420.

Building a Mirror Site

Two NAS systems are required, one as the SmartSync server, another as the SmartSync client. It will replicate data from the SmartSync client to the SmartSync server.

On the NAS system which acts as the SmartSync server, create a sync point in it. A sync point is a folder in the SmartSync server which is exposed to SmartSync clients for data replication. A sync point of mirror mode receives data from a SmartSync client and builds an identical data copy in it.

To create a sync point, please go to the **Backup➔SmartSync ➔Server** menu on the **Administration Page**. Click the **Add** button to open the page below. On the page you should provide the sync point name and specify which group is allowed to replicate data to this sync point. Set the mode to "**Mirror**".

SmartSync – NAS-to-NAS Data Replication

The screenshot shows the 'Add Sync Point' dialog in the SmartSync configuration interface. The dialog has tabs for 'Summary', 'Server', and 'Tasks'. The 'Server' tab is active, showing the following configuration:

- Path: /Server_Disc (with a 'Select Path' button)
- Sync Point Name: mirror-sync
- Sync Point Comment: build a mirror site
- Group Allowed: Admins (dropdown)
- Mode: Mirror (dropdown)
- Option: ☐ Generate transaction logs, ☐ Use advanced GFS media rotation scheme
- keep daily backups for 07 days
- keep weekly backups for 04 weeks
- keep monthly backups for 12 months

At the bottom are 'Apply' and 'Close' buttons.

On the NAS system which acts as the SmartSync client, set up a SmartSync task, which defines the schedule settings and the source folder.

To set up a SmartSync task, please go to the **Backup→SmartSync →Task** menu on the **Administration Page**. Click the **Add Task** button.

The screenshot shows the 'SmartSync Tasks' table in the SmartSync configuration interface. The table has columns for Task Name, SmartSync Server, Sync Point Name, Action, Schedule, and Status. Below the table are buttons for 'Add Task', 'Delete Task', 'Modify Task', and 'Test'. The 'Add Task' button is circled in red.

Task Name	SmartSync Server	Sync Point Name	Action	Schedule	Status
bbb	192.168.80.48	aaa	Mirror	02:05, Daily	Idle
backup_cit	192.168.80.48	backup	Backup	Immediately	Idle
test_rt	192.168.80.48	backup	Restore	Immediately	Idle
123	192.168.80.48	target	Mirror	Immediately	Idle

There are four steps to take when adding a SmartSync task.

Step 1 is to specify the IP address of the SmartSync server. Please enter the IP address of the NAS system where you

create the sync point. The second input box is for the port number. By default, port 873 is used to get remote SmartSync server information such as sync point names. If the port is remapped by a firewall or a NAT device, you must specify the remapped port number here.

Step 2 is to choose a sync point of **“Mirror”** mode in the SmartSync server. Please also provide a user account with the privilege to replicate data to the sync point.

Step 3 is to complete the task settings. On the page you should provide the task name, select the source folder to replicate, specify the schedule and configure the SmartSync options.

Step 4 is for confirmation, showing the brief information of the task settings.

Making Disk-to-disk Backups

Two or more NAS systems are required, one as the SmartSync server, the rest as the SmartSync clients. It will backup data from the SmartSync clients to the SmartSync server.

On the NAS system which acts as the SmartSync server, create a sync point of **“Backup”** mode, which receives data from SmartSync clients and creates data backups in it.

To create a sync point, please go to the **Backup→SmartSync→Server** menu on the **Administration Page**. Click the **Add** button to open the page below. On the page you should provide the sync point name and specify which group is allowed to replicate data to this sync point. Set the mode to **“Backup”**.

Server | Network | Volume | Security | Event | Status | Backup | Virus Scan |

Tape Backup | SmartSync | Loader/Writer | System Profiles |

Summary | Server | Tasks

Add Sync Point

- Path: /Server_Disc [Select Path](#)
- Sync Point Name: backup-sync
- Sync Point Comment: create backups
- Group Allowed: Admins
- Mode: Backup
- Option:
 - ☐ Generate transaction logs
 - ☒ Use advanced GFS media rotation scheme
 - keep daily backups for 07 days
 - keep weekly backups for 04 weeks
 - keep monthly backups for 12 months

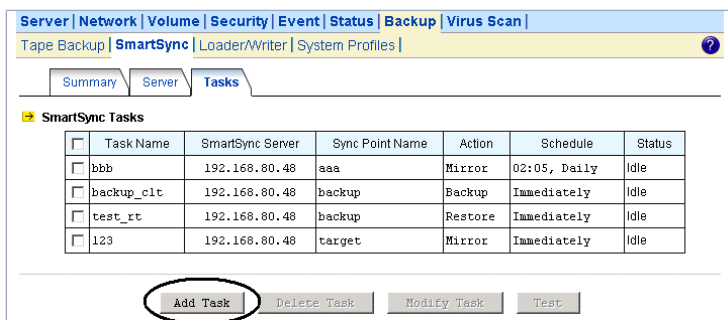
Apply Close

The GFS media rotation mechanism is the policy of managing backup versions. The policy is described as below. Basically it will check for obsolete versions and delete them when a new backup version is created. X, Y, Z are user-defined numbers.

- It will keep all the backup versions today.
- It will keep one backup version per day in the last X days, except today.
- It will keep one backup version per week in the last Y weeks prior to the X days.
- It will keep one backup version per month in the last Z months prior to the Y weeks.

On the NAS system which acts as the SmartSync client, set up a SmartSync task, which defines the schedule settings and the source folder.

To set up a SmartSync task, please go to the **Backup→SmartSync →Task** menu on the **Administration Page**. Click the **Add Task** button.



There are four steps to take when adding a SmartSync task.

Step 1 is to specify the IP address of the SmartSync server.

Step 2 is to choose a sync point of **"Backup"** mode in the SmartSync server. Specify the action as **"Backup to server"**. Please also provide a user account with the privilege to replicate data to the sync point.

Step 3 is to complete the task settings. On the page you should provide the task name, select the source folder to replicate, specify the schedule and configure the SmartSync options.

Step 4 is for confirmation, showing the brief information of the task settings.

Restoring Files from the SmartSync Backups

To restore data from the SmartSync server, please create a SmartSync task on the client. Open the **Administration Page** and enter the **Backup→SmartSync →Task** menu. Click the **Add Task** button.

Follow the steps to take to add the SmartSync task.

Step 1 is to specify the IP address of the SmartSync server.

Step 2 is to choose a sync point of **“Backup”** mode in the SmartSync server. Specify the action as **“Restore from server”**. Please also provide a user account with the privilege to replicate data to the sync point.

Step 3 is to complete the task settings. On the page you should provide the task name, select which backup version to restore, specify the target folder and configure the SmartSync options and the overwrite options. The overwrite options specify whether to overwrite the target with the files of the same names.

Step 4 is for confirmation, showing the brief information of the task settings.

Distributing File Updates to Multiple Sites

Two or more NAS systems are required, one as the SmartSync server, others as the SmartSync clients. It will replicate data from the SmartSync server to the SmartSync client.

On the NAS system which acts as the SmartSync server, create a sync point of **“Distribute”** mode, which distributes data to the SmartSync clients as they request.

To create a sync point, please go to the **Backup→SmartSync→Server** menu on the **Administration Page**. Click the **Add** button to open the page below. On the page you should provide the sync point name and specify which group is allowed to request data from this sync point. Set the mode to **“Distribute”**.

SmartSync – NAS-to-NAS Data Replication

The screenshot shows the 'Add Sync Point' configuration window. The 'Path' is set to '/Server_Disc' with a 'Select Path' button. The 'Sync Point Name' is 'distr-sync', and the 'Sync Point Comment' is 'distribute data'. The 'Group Allowed' is 'Admins' and the 'Mode' is 'Distribute'. Under 'Option', 'Generate transaction logs' is unchecked, and 'Use advanced GFS media rotation scheme' is checked. The rotation settings are: keep daily backups for 07 days, keep weekly backups for 04 weeks, and keep monthly backups for 12 months. 'Apply' and 'Close' buttons are at the bottom.

Server | Network | Volume | Security | Event | Status | Backup | Virus Scan |

Tape Backup | SmartSync | Loader/Writer | System Profiles |

Summary | Server | Tasks

Add Sync Point

- Path: /Server_Disc [Select Path](#)
- Sync Point Name: distr-sync
- Sync Point Comment: distribute data
- Group Allowed: Admins
- Mode: Distribute
- Option:
 - ☐ Generate transaction logs
 - ☒ Use advanced GFS media rotation scheme
 - keep daily backups for 07 days
 - keep weekly backups for 04 weeks
 - keep monthly backups for 12 months

Apply Close

On the NAS system which acts as the SmartSync client, set up a SmartSync task, which defines the schedule settings and the target folder.

To set up a SmartSync task, please go to the **Backup→SmartSync →Task** menu on the **Administration Page**. Click the **Add Task** button.

The screenshot shows the 'SmartSync Tasks' table. The 'Add Task' button is circled. The table has columns for Task Name, SmartSync Server, Sync Point Name, Action, Schedule, and Status. There are four tasks listed: 'bbb', 'backup_cit', 'test_rt', and '123'.

Server | Network | Volume | Security | Event | Status | Backup | Virus Scan |

Tape Backup | SmartSync | Loader/Writer | System Profiles |

Summary | Server | Tasks

SmartSync Tasks

<input type="checkbox"/>	Task Name	SmartSync Server	Sync Point Name	Action	Schedule	Status
<input type="checkbox"/>	bbb	192.168.80.48	aaa	Mirror	02:05, Daily	Idle
<input type="checkbox"/>	backup_cit	192.168.80.48	backup	Backup	Immediately	Idle
<input type="checkbox"/>	test_rt	192.168.80.48	backup	Restore	Immediately	Idle
<input type="checkbox"/>	123	192.168.80.48	target	Mirror	Immediately	Idle

Add Task Delete Task Modify Task Test

Follow the steps to take to add the SmartSync task.

Step 1 is to specify the IP address of the SmartSync server.

Step 2 is to choose a sync point of “**Distribute**” mode in the SmartSync server. Please also provide a user account with the privilege to request data from the sync point.

Step 3 is to complete the task settings. On the page you should provide the task name, select the target folder to receive data, specify the schedule and configure the SmartSync options.

Step 4 is for confirmation, showing the brief information of the task settings.

The SmartSync Options

When setting up a SmartSync task, you will see the following SmartSync options.

- **Compress the data stream during data transmission:** when checked, it will compress data before transmitting to the SmartSync server. Sometimes it will make it faster to complete a task. However, it takes extra CPU time to compress data and may have performance penalty if compression ratio is low.
- **Contain security information:** when checked, it will send ACL information to the SmartSync server.
- **Bandwidth control:** limits the maximum bandwidth for the task.
- **Include/exclude file pattern:** for excluding or including certain file types in the synchronization. For example, to exclude WORD files, type `*.doc`; . To exclude all WORD files except those beginning with abc, type `+abc*`; `*.doc`; .
- **Perform quick synchronization:** quick synchronization will only check file date, time and size when matching files, instead of checking block-by-block. It will speed up the synchronization a lot, while taking the risk that files might not be made identical.
- **Generate transaction logs:** when checked, it will record which files are added, updated or deleted during the

data replication. The transaction logs are displayed on the SmartSync **Summary** page.

9.6 Backup and Restore System Profiles

To recover from system failures, it requires restoring data and system configurations. Tape backup and SmartSync are for restoring data, while system profiles are used for recovering system configurations. System profiles are the backups of all system configurations, user database and security information.

Backing Up System Profiles

To back up system configurations, please open the administration page and go to **Backup→System Profile**. System profiles are saved manually or on a regular basis as defined on the page. System profiles will be saved locally on HD. The current backups are displayed on the lower page. To delete a system profile, check its check-box and click the **Delete** icon.

Recovering the system configurations when a disaster happens

If there is any system failure which causes corrupt system configurations, the first step is to reset the system configurations to factory default. Go to the **Server→Shutdown** page. Check the **Reset configuration to factory default** option and click the **Reboot** button.

The second step is to restore system configurations using one of the system profiles. Go to the **Backup→System Profiles→Restore** page. Select a system profile and choose which part of the system settings to restore. Then click the **Apply** button.

A system profile can also be created by the NASTart software. To recover from a system profile saved by NASTart, click the **An external file** item and find the system profile. Specify restore options and click the **Restore** button.

Restore options are:

- **Server, network and backup settings** – includes all settings in the **Server, Network, Backup** and **Event→Configuration** menus. Please note that the admin password will not be restored during the recovery.
- **User accounts and quota settings** – includes local accounts, current domain accounts and trust domain accounts, together with their quota settings. User accounts will be appended to the existing user database – local accounts with the same names will be overwritten; domain accounts with the same SID will be overwritten; others will be added to the existing user database.
- **Security Information, including network shares and ACLs** – includes all network shares, share permissions and access control lists.


Chapter 10 Event Logs and System Status

This chapter covers the Event Notification and System Status pages. You can collect information about the system, hardware and security event of you NAS system. NAS system records three kinds of logs:

- **System Log**
- **Device Log**
- **Security Log**

All the events are categorized into three levels: **Info**, **Warning** and **Error**. In **Event→Configuration** menu, you can configure the level of the logs. Use the **Advance** or **Basic** button to switch between the display of advance and basic information. The **Advance** view shows all the information in the Basic view plus additional event notification setting that may be of interest to the more advanced user. Various notification methods are provided by NAS system to ensure non-stop operation and data integrity:

- **LCD alert** – provides warning and error level notification:
 - Warning level notification such as very low disk space is detected on volume; hot spare disk is consumed and so on.
 - Error level notification such as CPU fan failed; volume is degraded or faulty and so on.
- **Web Reminder*** – provides instant notification in the administration homepage.
- **Email Alert*** – provides notification via email.
- **SNMP Trap*** – sends SNMP trap to the Network Manager System (NMS) such as HP Open View.
- **Buzzer Alert*** – an audio sound will goes off from the build-in buzzer in NAS system when event occurred. To turn off the buzzing sound, either

press any button on the LCD front-panel or click the **Mute Buzzer** icon  on the Administration Page.

* You can configure what kind of events should initiate the notification process in **Event→Configuration→Advance** menu.

10.1 Thermal Settings

User can also define the thermal scheme of the NAS system so that NAS system can give off warning message or shutting down when the system or CPU temperature is over a pre-defined threshold temperature.

Configuring thermal settings:

1. Go to **Thermal Settings** in **Event→Configuration** menu.
2. Enable **CPU Fan Control** if you want NAS system to adjust the CPU fan speed automatically based on the CPU and System temperature. Otherwise, the CPU fan will always run at full speed.
3. You can set the NAS system to give off warning message or shutdown base on the CPU or System temperature. Check the **Warning** and **Shutdown** checkboxes and select the proper temperature from the pull down menu.
4. Click **Advance** button to configure the way of notification for various events.
5. Click **Apply** to save the setting.

10.2 Checking the Event Logs

You can view a summary of all the events occurred on your NAS system: **Web Reminder, System Log, Device Log & Security Log**. The severity of each event will be determined by NAS system and displayed in different colors:

- Information = Green
- Warning = Yellow
- Error = Red



Viewing Web Reminder

Web Reminder is the warning message that appear at the first screen of the administrator home page to alert administrator that one or multiple critical events of your NAS system has been found. Administrator can, therefore be aware of the status of the NAS system immediately when entering the administrator home page. Click the hyper-link of the Web Reminder message and it will directly lead you to the Web Reminder summary menu.

Go to **Event→Web Reminder** menu to see a summary of all the critical events occurred on your NAS system.

Viewing System Log



In the **Event→System Log** menu, you can:

1. Select the number of most recent events show on a screen.
2. Select the severity level for the events you want to see.
3. Click **Refresh** or  button to refresh the screen.
4. Click **Clear** or  button to clear the log.

Viewing Device Log



In the **Event→Device Log** menu, you can:

1. Select the number of most recent events show on a screen.
2. Select the severity level for the events you want to see.

3. Click **Refresh** or  button to refresh the screen.
4. Click **Clear** or  button to clear the log.

Viewing Security Log

In the **Event→Security Log** menu, you can:

1. Select the number of most recent events show on a screen.
2. Select the severity level for the events you want to see.
3. Click **Refresh** or  button to refresh the screen.
4. Click **Clear** or  button to clear the log.
5. Select the protocols and click the **Refresh** button to show the corresponding events. **Default** event represent general security event of your NAS system that is not related to any protocols.

10.3 Viewing System Status

System Status displays a comprehensive view of the system fan status, thermal status and system voltage. You can use this information to quickly find out the problem of your NAS system and take appropriate action. In **Status→Environment** page, you can monitor the CPU fan status, CPU and System temperature plus the System Voltages. Click **Refresh** to obtain the latest figure.

Viewing the Open Files


In **Status→Open Files** menu, it provides the following information about all the open files on NAS system:

- **R/W** – read/write privileges of the opened file.
- **User** – the name of the user who has opened the file.
- **Protocol** - the protocol used for the network connection: SMB, NFS, AFP or FTP.
- **File Name** – lists the name and path of the opened file.

Viewing the Active Connections

In the **Status→Connections**:

- **Current Connections** – configure and show the protocol used by the client that is currently connecting to the NAS system by click the check box beside the protocol you want to show on the list.
- **User** – the name of the user who has connected to NAS system.
- **Computer** – the computer name of the client connecting to the NAS system.
- **Address** – the IP address of the client connecting to the NAS system.

- **Protocol** – the protocol used for the network connection: SMB, NFS, AFP or FTP.
- **Connected Time** – the date / time that the connection is established.
- **Open Files** – total number of the open files.
- **Disconnect** – disconnect a particular connection by check the disconnect check box and click the  icon.

10.4 Saving System Settings and Status as HTML Files

For maintenance or technical support purpose, it is helpful and sometimes necessary to have an overview of all system settings, current system status and, event better, all event logs. It also helps a lot if a server itself can send out these files by email.

The NAS system does all the above within several mouse-clicks.

First of all, you have to create a system folder, which is used for storing these files. The system folder is also required when performing tape backup jobs. To create the system folder, please open the **Administration Page** and go to the **Server→Maintenance** menu. On the menu page, select a volume to contain the system folder. And click **Apply** to create the system folder.

Once the system folder is created, you are able to save the system settings and event logs as HTML files. On the same page, choose the files to save and click the **Apply** button. Before saving the files, you can preview them by clicking the **Preview:** hyperlinks. Previewing will not create any files in the system folder.

After generating these files, you can see them appear in the table. Click any hyperlink to view the content of a file.

To email the save files, choose the files to save and check the **Send the saved files by email** check-box. Enter the email address to send to. And click **Apply** to send them out by email, while saving copies in the system folder.

This page is left blank intentionally

Chapter 11 Virus Protection

Most storage systems are vulnerable to virus attacks. An infected file in you NAS system can be exchanged among the clients system in the network and resulting in corrupted data or causing productivity loss. The integrated Trend Micro antivirus software in NAS system is the best-of-breed security product that delivers the reliable antivirus protection to prevent virus from spreading before they get to you.

The antivirus scanning software is optional on model 4100/8100. To activate it, you have to purchase a license key from the vendor. Please read Chapter 1 for how to activate the optional feature when you get the license key.

11.1 Information

The **Information** screen is the summary of the current antivirus settings. It gives you a comprehensive overview of the current status of antivirus general settings, real-time scans history and scan task summary of your NAS system. General settings display the present condition of the following items.

Real-time Scan	Display real-time scanning is either disabled or enabled
Virus Scan Schedule	Display schedule virus scanning is either disabled or enabled
Virus Scan Status	Display virus scanning is either idle or scanning.
Pattern Update Schedule	Display the status, schedule for the next virus pattern file update
Last successful update	Display the date/time of the last successful virus pattern file update
Scan engine version	Display the current scan engine version
Virus pattern version	Display the current virus pattern file version
Quarantine Folder	Display the folder name and path where virus infected files are

located and quarantine

The real-time scan history display the date time that the virus is found, virus name, action taken and the full path name of the infected file. And, the scan task summary display the start time of each manual or scheduled scan task.

11.2 Real-time, Manual and Schedule Scanning

The embedded antivirus utility provides several options for virus protection, including real-time, manual and scheduled scanning to offer comprehensive antivirus and content security solutions for enterprise customers.



Note:

Antivirus requires the system folder to operate. Please go to the **Server → Maintenance** page and specify the volume where the system folder resides.



Note:

For the first-time operation, please go to the **Virus Scan → Update** page to obtain the most updated virus pattern file. Otherwise, the antivirus function cannot work.

Enabling Real-time Scanning

The real-time scanning function provides antivirus protection while users are reading or writing files to the NAS system.

1. Click the **Enable Real-time scan** checkbox to enable real-time scanning.
2. Select scan direction. Incoming files are those that are being stored in NAS system whereas outgoing files are copied or moved from NAS system to other location.
3. Click **Apply** to save the settings.

Configuring Manual Scanning

The manual and scheduled scanning function can scan any folders for infected files. The scan results will be listed as a scan task summary on the **Information** page.

1. Go to **Virus Scan** → **Setting** page to configure the scan settings required. See “Configuring Scan Settings” on Section 10-3.
2. Click the **Manual** tab to go to the manual scanning page.
3. Click the **Select Folders** hyperlink to specify the folders you want to perform the manual scan.
4. Click **Apply** to save the settings.

Configuring Schedule Scanning

1. Click the **Enable Scheduled Scan For Infected Files** checkbox to enable scheduled scanning.
2. Click the **Select Folders** hyperlink to specify the folders you want to perform the scheduled scan.
3. Configure the start time and recurrence pattern for the scheduled scanning.
4. Click **Apply** to save the settings.

11.3 Configuring Scan Settings

All virus scan has two options that need to be configure.

- File Type to Scan – you can limit scanning to specific file types.
- Action When Virus Found – three actions (quarantine, clean, delete) can be chose from when virus is found.


File Types to Scan

The screenshot shows the 'File Types to Scan' configuration window. At the top, there is a navigation bar with tabs: Server, Network, Volume, Security, Event, Status, Backup, and Antivirus. Below this is a sub-navigation bar with tabs: Information, Scan, Setting, and Update. The 'Setting' tab is selected. The main content area is titled 'File Types to Scan'. It contains three radio button options: 'All file types', 'Files with specified file extensions ONLY' (which is selected), and 'Scan selected extensions'. Under the 'Files with specified file extensions ONLY' option, there is a sub-option 'Scan Trend Micro recommended extensions' with an 'Info' icon, and another option 'Scan selected extensions'. Below these options, there is a text input field labeled 'Type a file extension:' with a '>>' button to its right. To the right of the input field is a larger text area labeled 'List of selected file extensions:' with a '<<' button above it.

1. Click the desire scan file type.
2. If **All file types** is selected, all files regardless to its file extension will be scanned.
3. If **Files with specified file extensions Only** is selected, specify using the recommended extensions recommended by Trend Micro or specify the file extension manually.
4. Note that the maximum scanning layer of a compressed file is set to 2 layers for all real-time, manual and scheduled scan.

Actions When Virus Found

Configuring Scan Settings

 **Action When Virus Found**

☒ Quarantine: move infected files to the quarantine folder

☐ Clean: remove virus code from infected files

☐ Delete : remove infected files

Apply

1. Click the desire action when virus was found.
2. Click **Apply** to save the settings.

11.4 Updating Virus Pattern File

Virus pattern update can be performed either manually or according to the schedule. It is required to perform a manual update immediately when the antivirus function is activated for the first time.

Configuring a manual update

1. To download virus patterns from Internet, select **Trend Micro update server on internet**. Please note that you have to specify the DNS server IP address on the **Network→TCP/IP** menu of the Administration Page.
2. Or, you can download the virus pattern file in ZIP format from Trend Micro's website – <http://www.trendmicro.com> manually. Select **A virus pattern file in ZIP format** here and specify the location of the virus pattern file.
3. Click **Apply** to save the settings.

Configuring a scheduled update

1. Click the **Enable Scheduled Update of Virus Pattern Files** checkbox to enable scheduled update.
2. Configure the download schedule. Select the start time and recurrence pattern for the scheduled update.
3. Click **Apply** to save the settings.

This page is left blank intentionally

Chapter 12 Activating Optional Features

Optional software features of the NAS systems are disabled by default. You have to get a license key from your vendor and activate the optional features before you can use them.

12.1 Activating Optional Features

To activate the optional features, please follow the steps.

1. Open the **Administration Page**, select **License** from the **Server** menu. The page is like:

Server | Network | Volume | Security | Event | Status | Backup | Virus Scan |

Information | General | Password | UPS Settings | Maintenance | Shutdown | Upgrade | **License** | ?

■ The features below require license keys to activate. Please enter an appropriate license key or trial key in order to activate the related features.

➤ Feature List

Feature Name	License Type	Trial Period
Antivirus	Full	

- Enter the license key or trial key:

2. Enter the license key in the input field. A license key is a string of 24 characters. The characters can be any numbers or English letters. Please note that license keys are case-sensitive.
3. Click **Apply** to save the settings.
4. The activation is successful if the **License Type** becomes **Full**.



The page is left blank intentionally

Appendix A Specification



Hardware Specification for the 5.25" NAS Controller

Dimension	41x148x287mm (H x W x D)
Input Power	Standard ATX power connector 4100C/8100C: 3.3V: 3A 5V: 4A 12V: 0.5A 8200C: 3.3V: 4A 5V: 4A 12V: 1A
Operating Temperature	0 – 40 degree Celsius
Operating Humidity	10 – 80%, non-condensing
Regulatory Certifications	FCC Class A, CE

LED Indicators

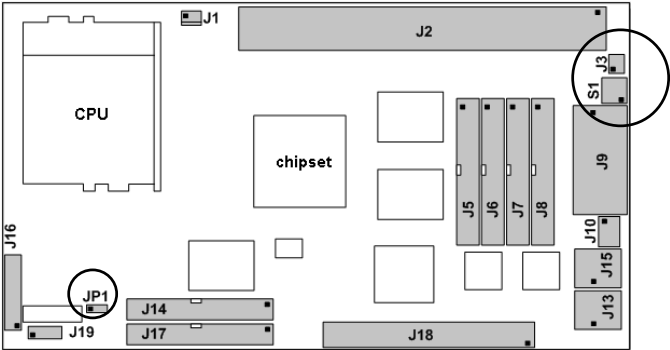
		On	Off	Blink
 LAN 1	Amber*	1000M link	no link	1000M activity
	Green	100M link	no link	100M activity
	Yellow	10M link	no link	10M activity
 LAN 2	Amber*	1000M link	no link	1000M activity
	Green	100M link	no link	100M activity

Hardware Specification for the 5.25" NAS Controller

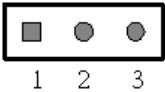
	Yellow	10M link	no link	10M activity
 HD Access	Red	–	–	IDE activity
 Power/Fault	Green	Power on	–	–
	Yellow	Fault	–	–

Note: Only available on Model 8200C.

Jumpers and DIP switch



JP1: (reset to default)

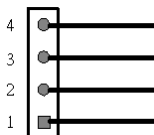


Pin Number	Function
Pin 1	PWR
Pin 2	SetDefault#
Pin 3	GND

Short Pin 1/2 => normal operation

Short Pin 2/3 => reset system configuration to factory default

J3: (power switch & reset switch)

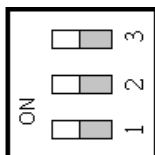


Pin Number	Function
Pin 1	PowerSwitch#
Pin 2	GND
Pin 3	ResetSwitch#
Pin 4	GND

Pin 1/2: connected to the system power switch.

Pin 3/4: connected to the system reset switch.

S1: (operation mode)



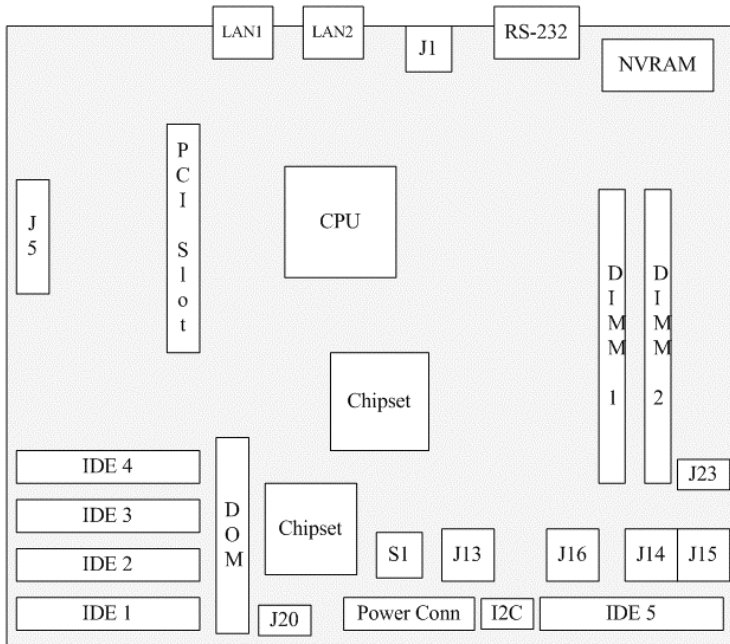
DIP 1	DIP 2	Operation Mode
ON	ON	Clear Password
OFF	ON	Manufacturing Use
ON	OFF	Network Recovery Mode
OFF	OFF	Normal

DIP 3	
ON	MR-423I not installed
OFF	MR-423I installed

Hardware Specification for 8400M NAS Main board

Dimension	Micro-ATX Form Factor 24.4cm(L) 24.4cm(W)
Input Power	Standard 400W ATX power connector 8400M: 3.3V: 8.8A 5V: 20A 12Vmax: 21.2A 12Vpeak: 28A
Operating Temperature	0 – 40 degree Celsius
Operating Humidity	10 – 80%, non-condensing
Regulatory Certifications	FCC Class A, UL, CE

Jumpers and DIP switch



- J1:** CPU Fan connector
J5: Front Panel connector
J13: System Fan #4 connector
J14: System Fan #2 connector
J15: System Fan #1 connector
J16: System Fan #3 connector

DIP 1	DIP 2	Operation Mode
ON	ON	Clear Password
OFF	ON	Manufacturing Mode
ON	OFF	Network Recovery Mode
OFF	OFF	Normal

DIP 3	Status
ON	Backplane not installed
OFF	Backplane installed

Hardware Specification for MR-423I Hotswap HDD module

Dimension	130x150x220mm (H x W x D)
Input Power	Standard ATX power connector. Power ratings depend on HDD.
Operating Temperature	0 – 40 degree Celsius
Operating Humidity	10 – 80%, non-condensing

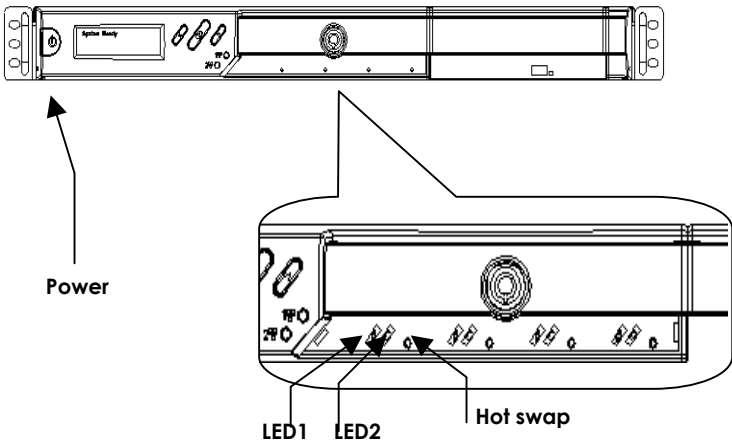
LED Indicators

LED 1 (Power/Fault)	LED 2 (HD Access)	Meaning
Green Blinks	Off (Master) Red On (Slave)	Powering up
Green On	Red On during access	HDD is being accessed
Green Blinks Fast	Red On	RAID building, rebuilding, expanding or disk-scanning
Amber On	Off	HDD is ready for being hot- unplugged
Amber Blinks Fast	Off	HDD carrier fan error. Blinking interval is about 0.5 second.
Amber Blinks Slowly	Off	Disk faulty. Blinking interval is about 2 seconds.
Green/Amber Interleaves	Off	IDE cable connect error
Off	Off	No power Hard disk is absent IDE cable is not connected

Hardware Specification for 1U Rack mount Model

Dimension	43.5x436x710mm (H x W x D)
Input Power	Standard ATX power connector. Power ratings depend on HDD.
Operating Temperature	0 – 40 degree Celsius
Operating Humidity	10 – 80%, non-condensing

LED Indicators

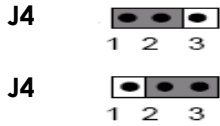


LED 1 (HD Access)	LED 2 (Power/Fault)	Power Switch	Meaning
Off (Master) Red On (Slave)	Green Blinks	X	Powering up
Red On during access	Green On	X	HDD is being accessed
Red On	Green Blinks	X	RAID building,

	Fast		rebuilding, expanding or disk-scanning
Off	Amber On	X	HDD is ready for being hot- unplugged
X	X	Amber On	Fan error.
Off	Amber Blinks Slowly	X	Disk faulty. Blinking interval is about 2 seconds.
Off	Green/Amber Interleaves	X	IDE cable connect error
Off	Off	X	No power Hard disk is absent IDE cable is not connected

J4: 3-pin HDD present jumper on the tray PCB board

Function	Jumper cap
HDD not present	Short pins 1-2
HDD present	Short pins 2-3 (default)



Hardware Specification for the Mini-Tower Model

Dimension	261x178x363mm (H x W x D)
Input Power	90 – 260V
Current Output for +5V	20A
Maximum Current Output for +12V	16A
Peak Current Output for +12V	28A
Output Wattage	370W

Hardware Specification for the 9-bay Tower Model

Dimension	430x175x490mm (H x W x D)
Input Power	90 – 260V
Current Output for +5V	20A
Maximum Current Output for +12V	16A
Peak Current Output for +12V	28A
Output Wattage	370W

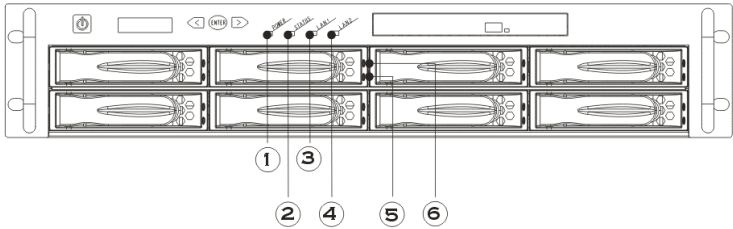
Hardware Specification for the 4U Rack Mount Model

Dimension	175x490x530mm (H x W x D)
Input Power	90 – 260V
Current Output for +5V	20A
Maximum Current Output for +12V	16A
Peak Current Output for +12V	28A
Output Wattage	370W

Hardware Specification for the 2U Rack Mount Model

Dimension	88x436x685mm (H x W x D)
Input Power	90 – 260V
Current Output for +5V	20A
Maximum Current Output for +12V	16A
Peak Current Output for +12V	28A
Output Wattage	370W

LED Indicators



Hardware Specification for the 2U Rack Mount Model

2: Fault LED

3: LAN1 LED

5: HDD Access LED

6: HDD ready LED

LED 6 (HD Access)	LED 5 (HDD Power)	Meaning
X	Green Blinks	Powering up
Red On during access	Green On	HDD is being accessed
Red On	Green Blinks Fast	RAID building, rebuilding, expanding or disk-scanning
Off	Amber On	HDD is ready for being hot-unplugged
Off	Amber Blinks Slowly	Disk faulty. Blinking interval is about 2 seconds.
Off	Green/Amber Interleaves	IDE cable connect error (PATA model)
Off	Off	No power Hard disk is absent IDE cable is not connected

This page is left blank intentionally

Appendix B Utility for NAS system

NASStart is a powerful software that discover and administer NAS Servers on the network, and remotely loads disc images into the NAS Server. You can either duplicate a whole CD or build an image from a group of files. Sharing and publishing data was never been so easy.

Use NASStart to display and modify the setting you have created. You can also perform server settings replication from a configured server to other NAS Servers on the network. Server parameters of a NAS Server can be imported into other NAS Server to avoid tedious setup process to each individual unit on the network.

Features:

Server Management -

- Discovers all NAS Servers on the network
- Configures NAS Servers for the first-time setup or quick setup
- Export / Import NAS Servers system settings

Creating CD Images Remotely -

- Remotely loads CD images from a local CD-ROM drive into a NAS Server
- Collect and duplicates files into NAS Servers as a single CD image
- Allows users to assign 6 different destination servers when building CD images
- Fully integrates the CD-R function of the NAS Server
- Supports up to 16 different tasks

User Interface -

- Explorer-like user interface together with user friendly wizards
- Task Manager monitors all on-going and scheduled tasks

Installation

System Requirement

- IBM PC or compatible with 80486 processor or higher
- At least 8 MB of free memory (16 MB is recommended)
- Minimum 5MB of free hard disk space
- VGA or higher resolution monitor
- Microsoft Windows 95/98/98SE/ME, Windows NT/2000/XP

Installing TCP/IP Protocol for Microsoft Networks

NASStart communicates with NAS Servers through the TCP/IP protocol. You must install **Client for Microsoft Networks** and the **TCP/IP** protocol in Windows to use NASStart.

Installing NASStart

You are ready to install this utility if the **TCP/IP** protocol is installed in your computer. To install NASStart, insert the Utility CD into the CD-ROM drive. On the auto-run interface, click "Install NASStart". If the auto-run interface does not appear, go to X:\NASStart and run **NASStart.exe**, where X is the drive letter of the CD-ROM drive.

Follow the instructions in the setup wizard to install NASStart. It will create shortcuts on **Desktop** and in the **Programs** folder of the Start menu.

Discovering NAS system

When startups, NASTart automatically discover all the NAS systems on the network and display a list of server under the node Local Server. NASTart will automatically refresh the server list at a specified interval. The default interval is 10 minutes.


NASTart can also locate NAS servers by IP addresses. It is useful when NAS servers are on the Internet or located in different network segments from the NASTart. To locate NAS servers by IP addresses, select **Remote NAS List** from the **File** menu. Click the **Add** button and enter the IP address of the NAS server.

To set the automatic refresh interval

1. Go to **Tool** → **NASTart Options** menu.
2. Enter a number between 1 to 60 minutes.
3. Click **OK**.

Server Quick Setup Using NASTart

You can perform initial setup for your NAS system using NASTart.

1. Click the  button on the toolbar.
2. Or, go to **Server** -> **Server Quick Setup**.
3. Select a NAS Server from the server list and click **Next** button.
4. Choose the **Network Teaming Mode** from the pull down menu. If you are not clear about this feature, continue with the default value. (Refer to Chapter 4.2 TCP/IP Settings)
5. If you want the IP settings to be assigned automatically, click **Obtain IP settings automatically**.
6. Or, you can specify the IP settings manually.
7. Click **Next** button to go to the next page.
8. Enter the **Server Name**, **Server Comment**, and **Workgroup/Domain Name** and select either the **Workgroup mode** or **Domain mode**. Note that this is the

server name as it appears on the network which is irrelevant to the network protocol used.

9. Click **Next** button to go to the next page.
10. Change the admin password if necessary.

Click the **OK** button to save the settings. Note that server may need to reboot for certain parameters changes to take effect.

Importing and Exporting System Settings

This section describes how to export the system settings of a NAS Server into a file. This file can be read into another NAS Server on the network by using the import feature. **Import System Settings** and **Export System Settings** form a combined process of replicate system settings from one configured NAS Server to another NAS Server.

To export system settings of a NAS Server

1. Highlight the server from the server list.
2. Right click the server and select **Export System Settings**.
3. Or, go to **Server -> Export System Settings** menu.
4. You will prompt for the administrator password to proceed.
5. Select a location where you want to save and specify the name of the export file.
6. Click **Save**.

To import system settings into NAS Servers

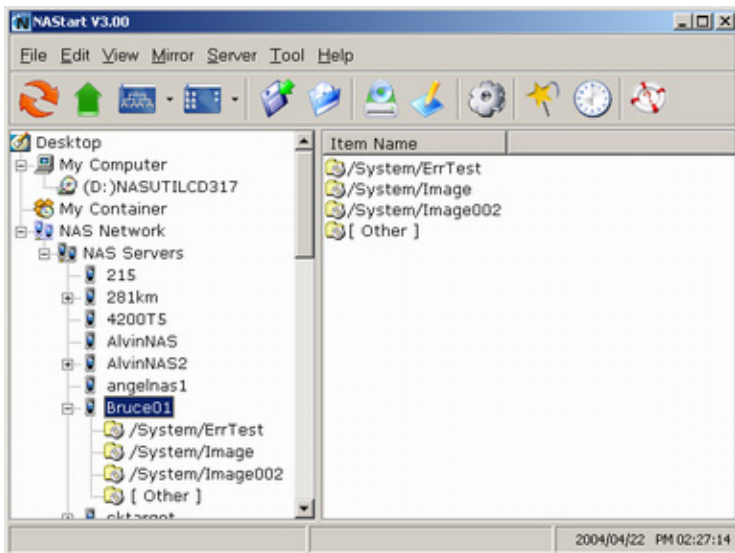
1. Right click any NAS Server and select **Import System Settings**
2. Or, go to **Server -> Import System Settings** menu.
3. You will prompt for the administrator password to proceed.
4. You have the option to select a server or an export file as the source.
5. Click **Next**.

6. Select the type of system settings you want to import into the target server. The detail content of the system settings are displayed in the preview text box beside each selection.
7. Click **OK**. NAS Server will reboot automatically.

Browsing & Administering Servers

Browsing Servers

Below is the main window of NASTart. Upon execution, NASTart brings up Windows Explorer for you to drag & drop files into My Container for later image building. You can disable this option by choosing **Tool->NASTart Options** and un-checking the option - "Open Windows Explorer when NASTart starts".



The main window consists of a file menu, a tool bar, a tree view pane on the left, a list view pane on the right and a status bar on the bottom.

On the tree view pane are listed all the NAS Servers found by the NASTart on the network. Also included is **My Computer** as the one in Windows Explorer. **My Container** keeps information of the files/folders that can be built as a CD image in a NAS Server using the "Build Image" function. If you click on any item

on the tree view pane, its content will be displayed in the list view pane.

The status bar indicates NASStart status & information. The left of the status bar shows function hint or item properties. To the right it displays the PC date and time.

You can browse the Domain Name, IP Addresses of each NAS Server just by mouse over it.

Note:

If a NAS Server is protected by the admin password, you have to enter the password to set up or write to the server.

The following are some icon representations:



NAS Network: display all the NAS Servers found on the LAN.



NAS Server: represents a NAS Server



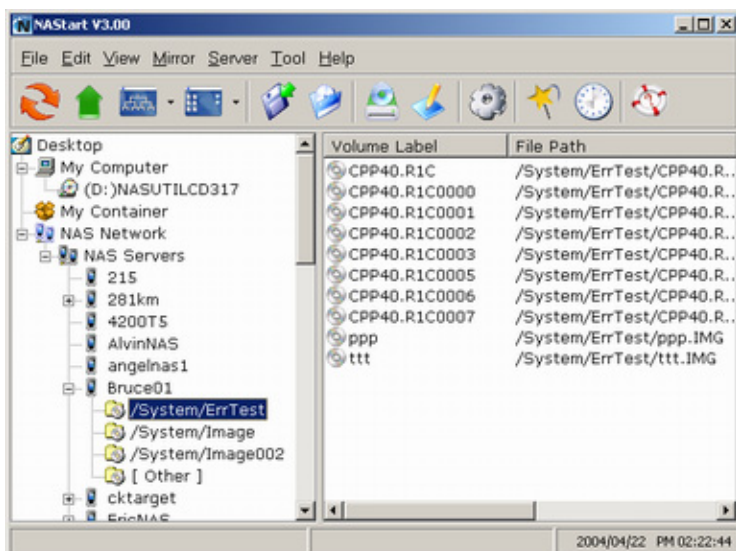
Disc Image Folder: contains disc images of the NAS Server. You can double click to view its content.



Disc Image: represents a mirrored CD/DVD image.

The following are some examples of browsing the servers.

Example 1. Content of a disc image folder



It displays all the disc images, path name, size, status and file system.

Tool Bar Functions

The tool-bar provides an easy access to the main functions of NASTart. The following explains what the tool-bar icons represent.



Refresh: manually updates the directory content of My Computer or NAS Network.



Up Directory: moves the cursor one level up.



Tree View Mode: expands or shrink the directory tree in the tree view pane (to the left).



List View Mode: changes the view mode of items in the list view pane (to the right).



Save Container: saves data in My Container into a container file.



Load Container: loads a container file into My Container.



Mirror CD: starts the "Mirror CD" wizard for duplicating CD images into the NAS Server.



Build Image: starts the "Build Image" wizard to build a CD image from My Container into a NAS Server.



Server Quick Setup: configures some fundamental parameters of a selected NAS Server. You can configure an un-initialized or initialized server.



Wizard: brings up a wizard for access to major functions: "Mirror CD", "Build Image" and "Server Quick Setup".



Task Manager: opens a task manager window which displays and controls all ongoing and scheduled tasks.




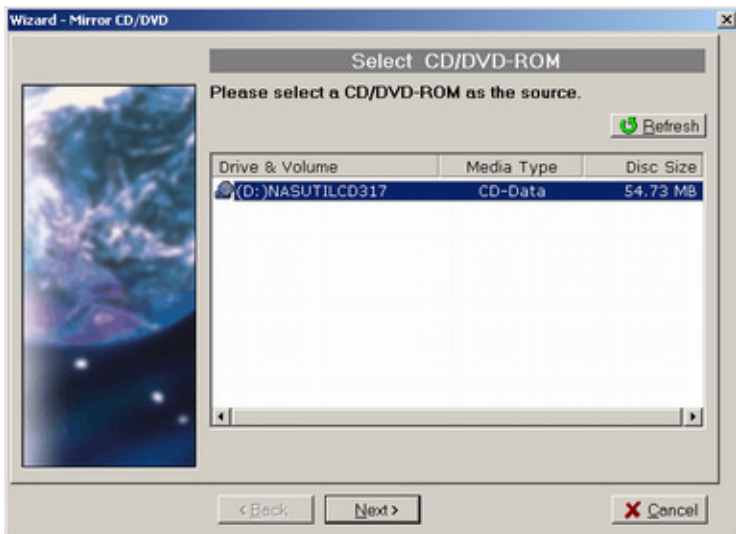
Help: opens the Help window for display help information.


Mirroring CD/DVD Remotely

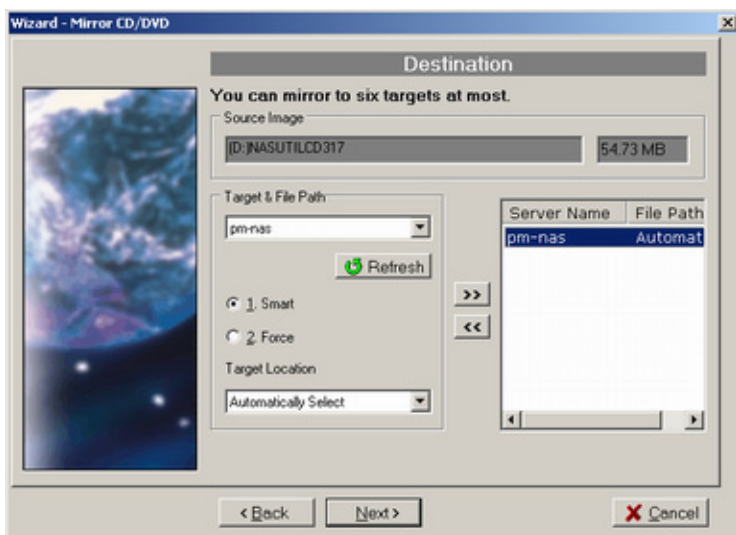
This chapter describes how to copy a CD from a PC CD-ROM drive to a NAS Server. Please follow the steps below.

1. To mirror a CD or a DVD remotely into a NAS Server, first

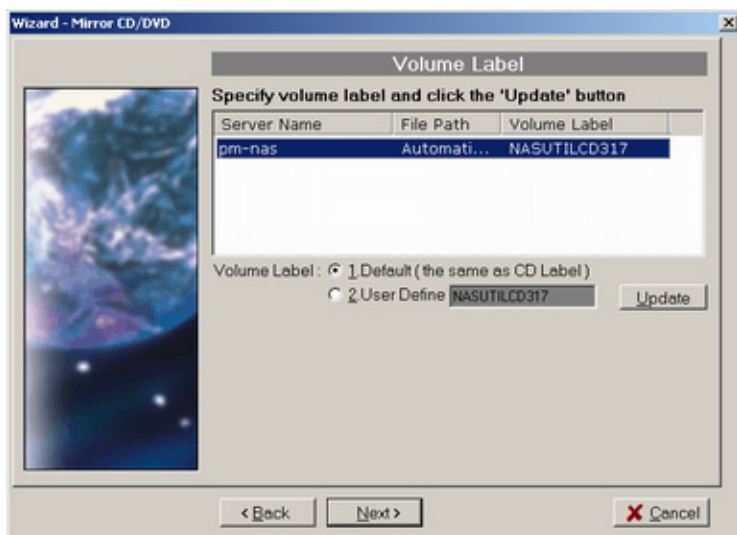
click the  "Mirror CD" icon on the tool-bar. It invokes the "Mirror CD" wizard as shown below. Select a PC CD-ROM drive as the source. Press **Next** to continue.



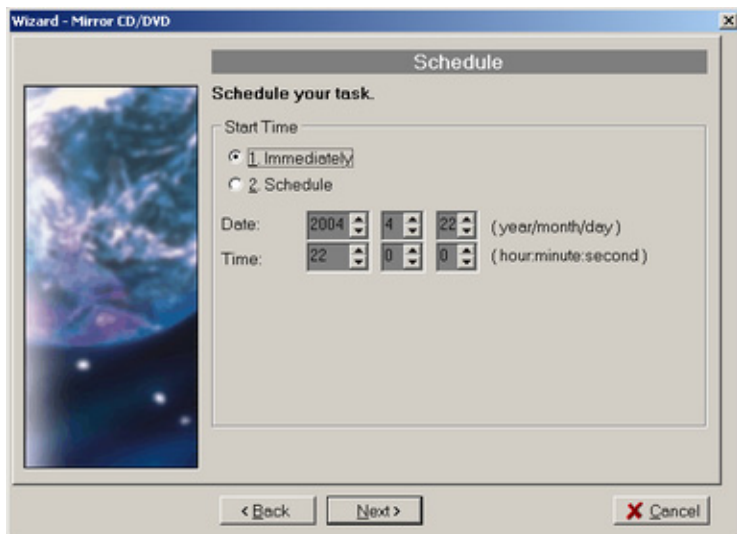
2. Choose one or more servers as the destination. Select a server in the **Target & File Path** list-box, select **Smart** mode for redundancy check of the CD image or select **Force** mode to allow a second copy of the same CD image. Then, click the  button. You can see the task being added to the right-hand pane. Click the **Next** button to go to next page.



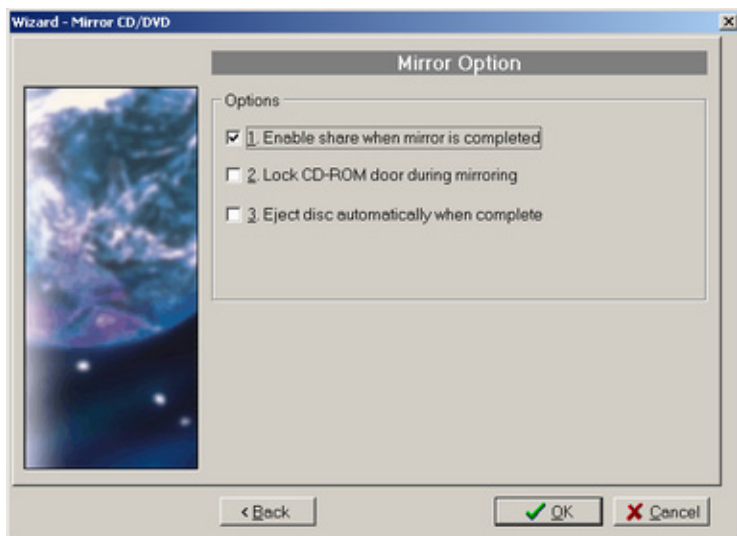
3. Change the volume label of the CD/DVD image if necessary. If you want to change the volume label, click the **2. User Define** radio button and enter the volume label in the input-box. Then click the **Update** button. Click the **Next** button afterwards.



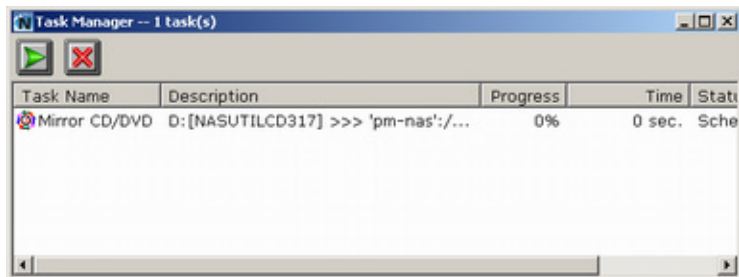
4. Specify the date/time to run the task. Then press **Next**.



5. Set the Mirror CD options if necessary.



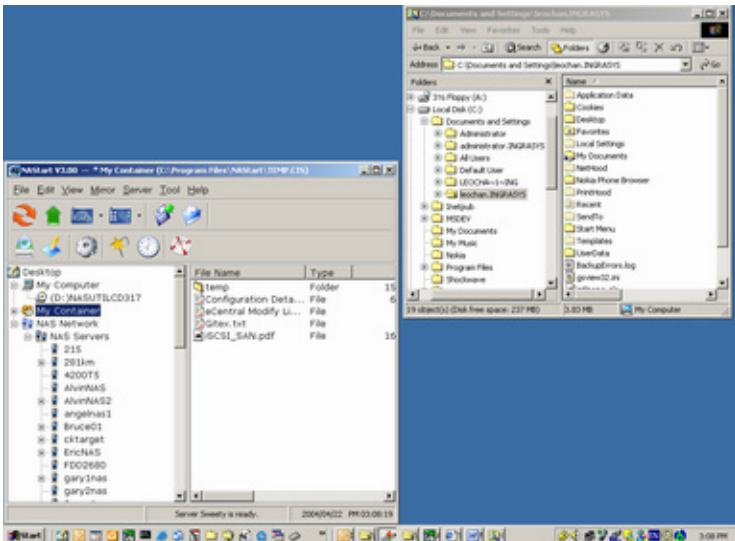
6. Click **OK** to start the task. The Task Manager will show the progress.



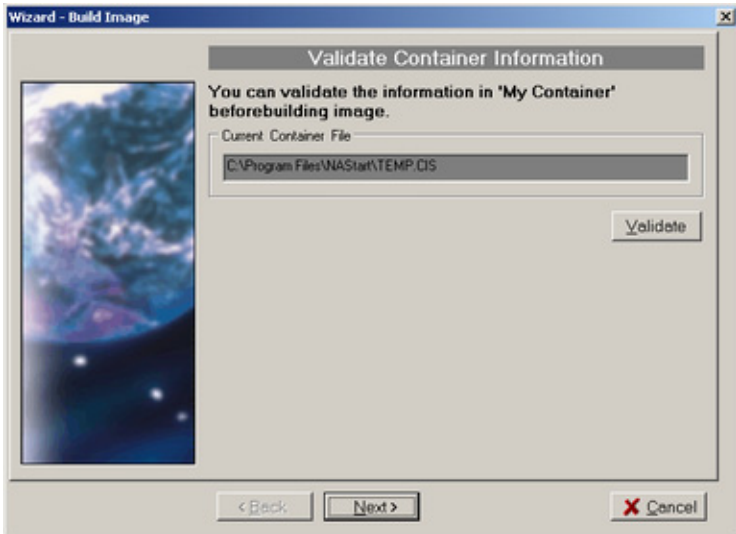
Archiving Files As a CD/DVD Image

This chapter describes how to build CD image from **My Container** into a NAS Server. Please follow the steps below.

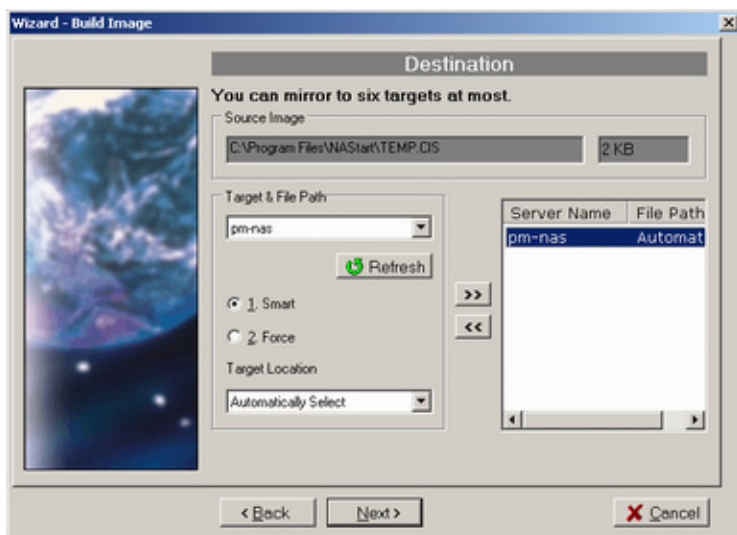
1. The first thing to build a CD/DVD image is to collect files. Open Windows Explorer and drag & drop files into My Container.



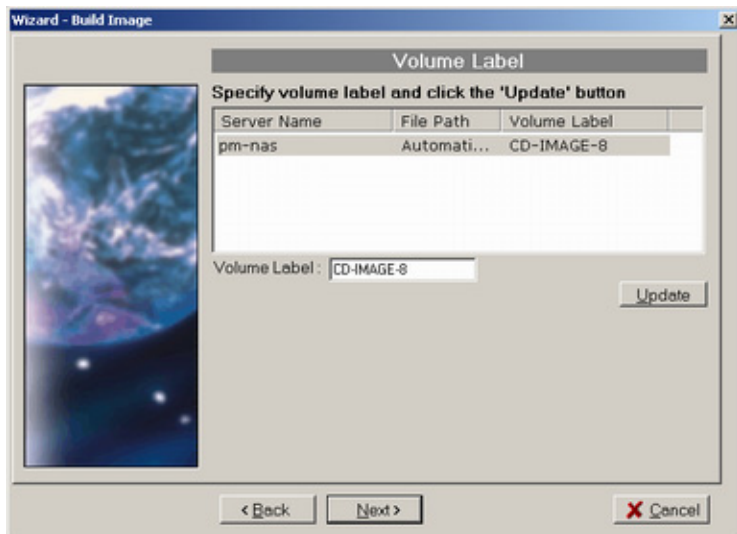
2. Click the  "Build Image" icon on the tool-bar to bring up the "Build Image" wizard. You can click the **Validate** button to check if the file/folder information in My Container is correct. If not, you can choose to update My Container.



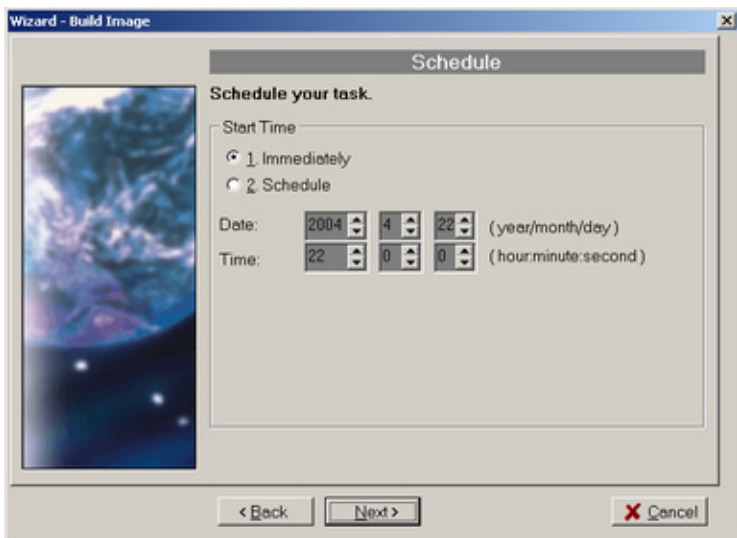
3. Choose one or more servers as the destination. Select a server in the **Target & File Path** list-box, select **Smart** mode for redundancy check of the CD image or select **Force** mode to allow a second copy of the same CD image. Then, click the **>>** button. You can see the task being added to the right-hand pane. Click the **Next** button to go to next page.



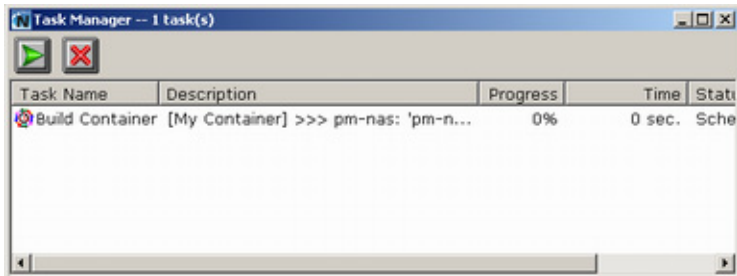
4. Name the CD/DVD image to be created. Enter the name in the **Volume label** input-box and click the **Update** button. Press **Next** afterwards.



5. Specify the date/time to run the task. Then press **OK**.



6. The Task Manager will show the progress.



Burning Disc Images

If the NAS server is equipped with CD or DVD writer, it can burn any existing disc image in it. Select a NAS server from the **NAS Servers** tree view pane of the NASTart main window. Select a disc image in the NAS server and right-click on it. Select **Record CD/DVD** from the right-click menu.

Specify the parameters in the wizard and click the **Add CD-R Option** button. Click **Next** to continue. On the next page, specify the launch schedule and click **OK**.

Supported CD Formats

The "Mirror CD" function copies CD or DVD discs from a PC CD/DVD drive into a NAS Server. Below is a list of the supported CD formats that can be mirrored remotely.

- ISO 9660 level 1, 2, 3 (including Romeo, Joliet and Rock-Ridge extension)
- CD HFS
- CD/DVD UDF
- High Sierra
- Hybrid (ISO+HFS)
- Multi-session CD
- Mixed Mode CD
- UDF V1.5, V2.0